ALEOS 4.4.0 Software Configuration

User Guide

SIERRA WIRELESS®

4116359
Rev 1

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the Sierra Wireless modem are used in a normal manner with a well-constructed network, the Sierra Wireless modem should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Sierra Wireless accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the Sierra Wireless modem, or for failure of the Sierra Wireless modem to transmit or receive such data.

Safety and Hazards

Do not operate the Sierra Wireless modem in areas where blasting is in progress, where explosive atmospheres may be present, near medical equipment, near life support equipment, or any equipment which may be susceptible to any form of radio interference. In such areas, the Sierra Wireless modem **MUST BE POWERED OFF**. The Sierra Wireless modem can transmit signals that could interfere with this equipment.

Note: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. Sierra Wireless modems may be used at this time.

The driver or operator of any vehicle should not operate the Sierra Wireless modem while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some states and provinces, operating such communications devices while in control of a vehicle is an offence.

Limitation of Liability

The information in this manual is subject to change without notice and does not represent a commitment on the part of Sierra Wireless. SIERRA WIRELESS AND ITS AFFILIATES SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUE OR ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE ANY SIERRA WIRELESS PRODUCT, EVEN IF SIERRA WIRELESS AND/OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR THEY ARE FORESEEABLE OR FOR CLAIMS BY ANY THIRD PARTY.

Notwithstanding the foregoing, in no event shall Sierra Wireless and/or its affiliates aggregate liability arising under or in connection with the Sierra Wireless product, regardless of the number of events, occurrences, or claims giving rise to liability, be in excess of the price paid by the purchaser for the Sierra Wireless product.

Patents

This product may contain technology developed by or for Sierra Wireless Inc. This product includes technology licensed from QUALCOMM®. This product is manufactured or sold by Sierra Wireless Inc. or its affiliates under one or more patents licensed from InterDigital Group and MMP Portfolio Licensing.

Copyright

© 2014 Sierra Wireless. All rights reserved.

Trademarks

Sierra Wireless®, AirPrime®, AirLink®, AirVantage® and the Sierra Wireless logo are registered trademarks of Sierra Wireless.

Windows® and Windows Vista® are registered trademarks of Microsoft Corporation.

Macintosh® and Mac OS X® are registered trademarks of Apple Inc., registered in the U.S. and other countries.

QUALCOMM® is a registered trademark of QUALCOMM Incorporated. Used under license.

Other trademarks are the property of their respective owners.

Contact Information

International Contact Information

Please contact your AirLink Reseller for technical support.

AirLink Sales	airlinksales@sierrawireless.com
AirLink Support	support@sierrawireless.com
AirLink RMA Repairs	repairs@sierrawireless.com
AirLink Online Support Knowledgebase	www.sierrawireless.com/Support/SupportCenter
AirLink Software Downloads	www.sierrawireless.com/Support/Downloads
Corporate Web Site	www.sierrawireless.com

Sierra Wireless Headquarters Contact Information

Postal Address:	Sierra Wireless 13811 Wireless Way Richmond, BC Canada V6V 3A4

Consult our website for up-to-date product descriptions, documentation, application notes, firmware upgrades, troubleshooting tips, and press releases:

www.sierrawireless.com

Contents

Introduction 13

Overview 13

Sierra Wireless AirLink Products 13

About Documentation 14

Tools and Reference Documents 15

Device Configuration 17

Toolbar 18

Configuring your AirLink Device 18

Saving a Custom Configuration as a Template 19

Applying a Template 21

SSH PAD Mode 23

Server Configuration 24

Update the ALEOS Software and Radio Module Firmware 30

Step 1—Planning Your Update 30

Recommendations 31

Step 2—Update the ALEOS Software and Radio Module Firmware 31

Updating Only the Radio Module Firmware 36

Enterprise LAN Management 37

Configuring Your Device for use in a PCI Compliant System 38

Status 41

Home 41

WAN/Cellular 49

LAN 62

Wi-Fi 63

VPN 65

Security 66

Services 67

GPS 68
Serial 69
Applications 72
About 73

WAN/Cellular Configuration 75
SIM PIN 93
Enable the SIM PIN 93
Change the SIM PIN 94
Disable the SIM PIN 95
Unblocking a SIM PIN 95
Re-Activation 96
Backup APN 96
Bandwidth Throttle 97
Reliable Static Routing (RSR) 100
Dynamic Mobile Network Routing (DMNR) 105

LAN/Wi-Fi Configuration 111
Private and Public Mode. 111
DHCP/Addressing 112
Ethernet 117
USB 119
Installing the USB Drivers 121
Host Port Routing 128
Wi-Fi 129
Access Point Mode 130
Client (Wi-Fi WAN) Mode 134
Both (AP + Client) Mode 138
Global DNS. 139
PPPOE 141
Configure the AirLink Device to Support PPPoE 142
Configuring a PPPoE Connection in Windows 7 143
VLAN 146

VRRP 148
Host Interface Watchdog 152

VPN Configuration 155
IPsec 155
Split Tunnel. 156
VPN 1 157
IPsec 157
GRE 162
SSL Tunnel 163
VPN 2 to VPN 5 167

Security Configuration 169
Solicited vs. Unsolicited 169
Port Forwarding 169
DMZ 173
Port Filtering—Inbound 175
Port Filtering — Outbound 176
Trusted IPs—Inbound (Friends). 177
Trusted IPs—Outbound 178
MAC Filtering 178

Services Configuration 181
AVMS (AirVantage Management Service) 181
ACEmanager 184
Low Power 186
Dynamic DNS 191
Understanding Domain Names 196
Dynamic Names 196
Wi-Fi Landing Page 197

SMS Overview 198
Sending SMS Commands to an AirLink Device 199
SMS Modes 200
Password Only 200
Control Only 201
Gateway Only 202
Control and Gateway 208
SMS Wakeup 210
SMS Security 211
Inbound SMS Messages 211
Trusted Phone Number 212
SMS Password Security 213
SMS > Advanced 214
SMSM2M 216
Telnet/SSH 217
Email (SMTP) 218
Management (SNMP) 220
Time (SNTP) 225
Authentication 226
LDAP Authentication 227
RADIUS Authentication 228
TACACS+ Authentication 229
Device Status Screen 231

GPS Configuration 233
GPS Overview 233
ALEOS Supported GPS Report Protocols 234
Before Configuring GPS 234
Servers 1 to 4 235
Local/Streaming 247
Local/Streaming—Local IP Report 249
Global Settings 253

Events Reporting Configuration 257
Introduction. 257
Additional Behavior and Features 258
Configuring Events Reporting. 258
Action Types 260
Report Data Group 267
Relay 270
Event Types 271

Serial Configuration 275
Port Configuration. 275
Port Configuration 276
Reverse Telnet/SSH 279
UDP Multiple Unicast 281
Advanced 282
TCP 284
UDP 286
PPP 288
Modbus Address List 289
I/O X-Card Serial Port Configuration 290
Advanced Settings 293
TCP Settings 294
UDP Settings 296
Configuring IP to Serial with Auto Answer and Serial to IP 298
LED Indicator 302

Applications Configuration 303
Data Usage. 303
Garmin 311
ALEOS Application Framework 314

I/O Configuration 317
AirLink GX Series device 317
AirLink LS300 317
Analog inputs 317
Digital inputs 318
Relay outputs 318
Current State 318
Pulse Count 320
Configuration 321
Transformed Analog 322

Admin 325
Change Password 325
Advanced 325
Radio Passthru 329
Log 330

Windows Dial-up Networking (DUN) 333
Installing a Device Driver 333
Creating a Dial-Up Networking (PPP) Connection 343
Connecting to the Internet Using DUN 352
ACEview 352
Windows DUN 353

Modbus/BSAP Configuration 355
Modbus Overview 355
Configuring the AirLink Device at the Polling Host for Modbus on UDP 357
Configuring the Remote AirLink Devices for Modbus with UDP 358

SNMP: Simple Network Management Protocol 361
Management Information Base (MIB) 361
SNMP Traps 361
Sierra Wireless MIB 361

AT Commands 387
AT Command Set Summary. 387
Reference Tables 388
Device Updates 389
Status 389
WAN/Cellular 395
LAN/Wi-Fi 401
LAN 401
Wi-Fi 403
VPN 407
Security. 412
Services 413
GPS 422
Serial 429
Standard (Hayes) commands 436
I/O. 442
Applications 443
Admin 444

SMS Commands. 447
SMS Command format. 447
List of SMS Commands 448

Q & A and Troubleshooting 451
ACEmanager Web UI 451
Ethernet Ports 451
LAN Networks 452
Wi-Fi 452
Port Forwarding 452
ALEOS Application Framework (ALEOS AF) 453
SMS 453
GPS 454
VPN 454
Poor Wireless Network Connection 456
Connection not working 456
Updating the ALEOS Software and Radio Module Firmware 457
TCP Connections 461
AirVantage Management Service 462
LTE Networks 463
SIM Card is Blocked 465
Remote connections 465
Radio Band Selection 465
Reliable Static Routing (RSR) 466
Inbound Ports Used by ALEOS 466
Event Reporting 467
TCP/IP and UDP/IP Auto Answer 467
Templates 469

Glossary of Terms 471

Index 477

1: Introduction

1

Note: This user guide is intended for the AirLink LS300 and the AirLink GX Series devices. If you have an AirLink ES440, refer to the ALEOS Software Configuration User Guide for the AirLInk ES440.

Overview

ACEmanager™ is the free, web-based utility used to manage and configure the AirLink® device. It is a web application integrated in the ALEOS™ software that runs on the AirLink device. AirLink Embedded Operating System (ALEOS) is purpose-built to maintain a wireless connection and to configure the gateway to the needs of the system. ACEmanager provides comprehensive configuration, monitoring, and control functionality to all AirLink gateways and routers.

ACEmanager enables you to:

- Login and configure device parameters
- Adjust network settings
- Change security settings
- Update events reporting and control outputs
- Update ALEOS software and radio module firmware
- Copy configuration settings to other AirLink devices

Since ACEmanager can be accessed remotely over-the-air as well as locally, the many features of ALEOS can be managed from any location.

An ALEOS configuration template can be created using ACEmanager, after a single device is configured and installed, to program other AirLink gateways with the same configuration values. This enables quick, accurate deployment of large pools of devices.

Sierra Wireless AirLink Products

ACEmanager is intended to be used with the following products with ALEOS:

- AirLink GX Series
- AirLink LS300
- AirLink ES440

Choosing the right product for your needs

	AirLink ES440	AirLink GX Series	AirLink LS300
Target	Enterprise (office, remote store, point-of-sale, etc.)	Mobile and Industrial (police, fire, fleets and oil, gas, rail, remote access)	Industrial (oil and gas utilities, remote solar panels)
Location	No GPS	GPS	GPS
Ingress Protection	n/a	IP64	n/a
Hazardous Location	n/a	Class 1 Div.2	Class Div. 2
Operating Temperature	-20° to 60°C	-30° to +70°C	-30° to +70°C
Shock and Vibration	1 m drop test, non-operational	Military Standard 810	Military Standard 810
Serial Features	Serial port: Reverse Telnet for OOBM	Serial Byte protocol support (DNP3, Modbus, BSAP, DF1 [Allen-Bradley])	Serial Byte protocol support DNP3, Modbus, BSAP, DF1 [Allen-Bradley])
Power	AC power only (9–36VDC)	AC and DC power (9–36VDC)	AC and DC power
Input/Output	No optional I/O	Optional I/O	Limited I/O
Events Reporting	SNMP Trap events only	Full Events Reporting, SMS Events Reporting	Full Events Reporting, SMS Events Reporting
Warranty	3 Year Warranty	5 Year Warranty	3 Year Warranty

For more information on specific AirLink products, refer to the hardware user guide, available from www.sierrawireless.com/en/Support/Downloads.aspx.

About Documentation

Each chapter in the ALEOS Configuration User Guide describes a section (a tab in the user interface) of ACEmanager.

Chapters in this user guide explain:

- Parameter descriptions in ACEmanager
- Relevant configuration details
- User scenarios for certain sections in the guide.

This User Guide is kept up to date and provided as a PDF (Portable Document Format) file on the Sierra Wireless support website.

Tools and Reference Documents

Document	Description
AirLink Device User Guide	This hardware document describes how to: • Install the AirLink device hardware • Connect the radio antennas • Connect a notebook computer and other input/output (I/O) devices • Interpret the LEDs and indicators on the AirLink device.
ACEview User Guide	This document explains how to use the ACEview utility to monitor the connection state of a Sierra Wireless AirLink device and GPS or power status as applicable.
AVMS User Guide	This document explains how to use AirVantage Management Service for the remote management of Sierra Wireless AirLink devices.

2: Device Configuration

To access ACEmanager:

1. Insert the SIM card, if applicable. Refer to the AirLink device user guide for details.
2. Power on the AirLink device.
3. Launch your browser and enter the IP address and port number http://192.168.13.31:9191

   ACEmanager is supported on the latest versions of Internet Explorer® and Firefox®.
4. Log in:
   - User Name: “user” (entered by default) or “viewer

     Use the “user” login for configuring or monitoring your device.

     Logging in as “viewer” only allows you to view the configuration and connection state. You cannot make any configuration changes.
   - Default Password: 12345

Note: ACEmanager has a default session idle timeout of 15 minutes. If there is no activity for the idle timeout period, you are redirected to the login screen. To change the session idle timeout period, see ACEmanager Session Idle Timeout (minutes) on page 184.

To prevent others from changing the AirLink device settings, you can change the ACEmanager password (Chapter 14).

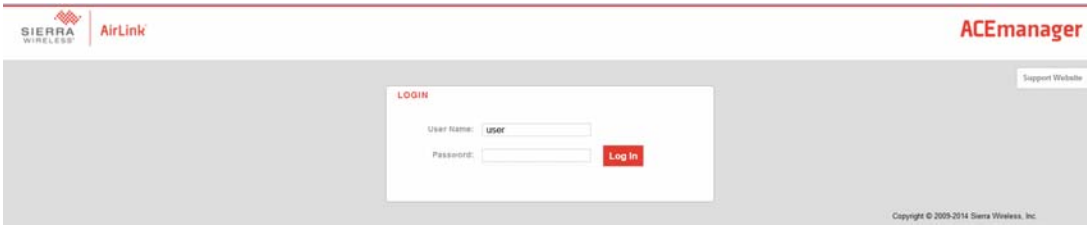


Figure 2-1: ACEmanager: Main Login screen

After your initial login to ACEmanager, you have the option of displaying the device status parameters on subsequent login screens.

5. In ACEmanager, go to Services > Device Status Screen.
6. In the Device Status on Login Screen field, select Enable. (For details, see Device Status Screen on page 231.)

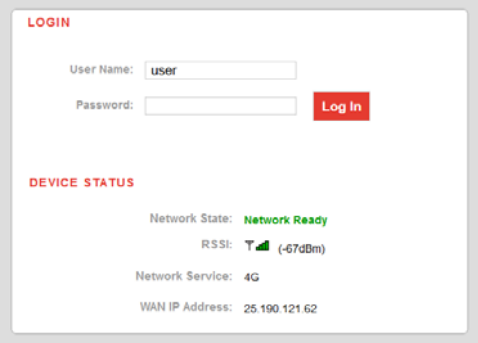
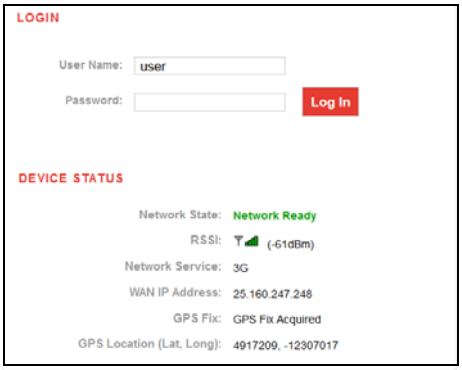


Figure 2-2: ACEmanager: Main Login screen with Device Status

If you have GPS fields selected on the Device Status screen, but GPS is disabled, the device login screen will show GPS Service Disabled.



Toolbar

The buttons on the ACEmanager toolbar are:

- Software and Firmware: Updates the ALEOS software and the radio module firmware
- Template:
  - Download and save a configuration as a template
  - Upload a saved template to apply settings
- Reboot: Reboots the device
- Refresh All: Refreshes all ACEmanager pages

Configuring your AirLink Device

There are three options for configuring the AirLink device:

- Use your browser-based ACEmanager (as detailed in this guide); or
- Use a terminal emulator application (e.g., Tera Term, PuTTY, etc.) to enter AT commands for many of the configuration options.
- Use the cloud-based AirVantage Management Service application (see www.sierrawireless.com/productsandservices/AirVantage_M2M_Cloud.aspx for more details.)

Saving a Custom Configuration as a Template

If you have a device configured to match your requirements, you can use ACEmanager to download and save that device's configuration as a template and then apply it to other Sierra Wireless AirLink devices.

To download and save a custom configuration as a template:

1. Connect a laptop to the device with the configuration you want to save as a template.
2. In ACEmanager, click the Template button on the toolbar.

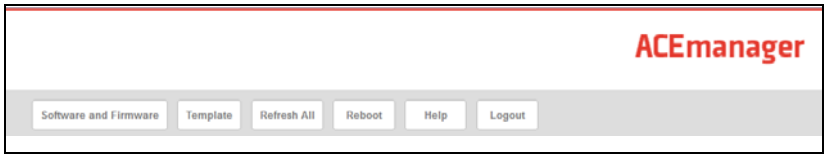


Figure 2-3: ACEmanager: Template button

The following window appears:

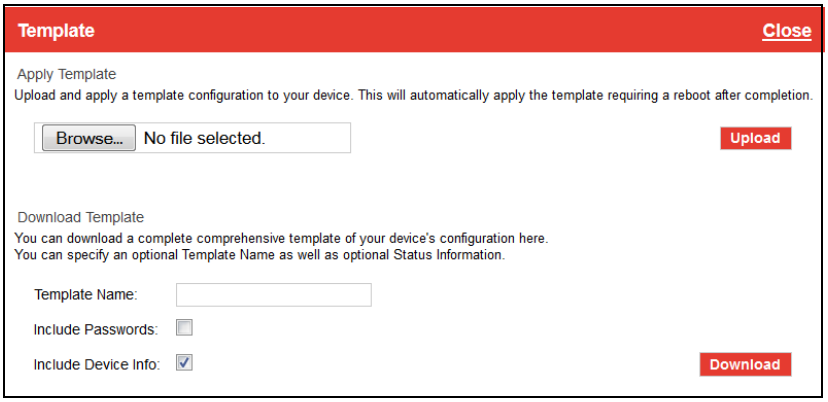

Template
Close
Apply Template
Upload and apply a template configuration to your device. This will automatically apply the template requiring a reboot after completion.
Browse...
No file selected.
Upload
Download Template
You can download a complete comprehensive template of your device's configuration here.
You can specify an optional Template Name as well as optional Status Information.
Template Name:
Include Passwords:
Include Device Info:
Download

Figure 2-4: ACEmanager: Template window

Use the bottom half of the window to download and save a template.

3. If desired, enter a Template Name. The file is saved using this name and a .xml file extension. Spaces and special characters are not supported, and if entered, are deleted from the file name.

   If no Template name is entered, the file is saved as SWIApplyTemplate.xml.

4. Choose whether or not to:
   - **Include Passwords**
     When Include Passwords is selected, passwords configured in ACEmanager (such as the email password, the SMS ALEOS Command password, the Serial PPP password, etc.) are shown in plain text in the template file. When the template is uploaded to a device, the passwords are included and replace any existing password configured on the device.
     If Include Passwords is not selected, password fields are not included in the

template file, and existing passwords persist when the template is uploaded to a device.

Note: The ACEmanager login password is not included when you select the Include Passwords option.

- **Include Device Info** (selected by default)
  When selected, the template file includes a “snap-shot” of the current Status tab information with the current settings. This could be useful for troubleshooting.

5. Click Download. The download status appears at the bottom of the window.

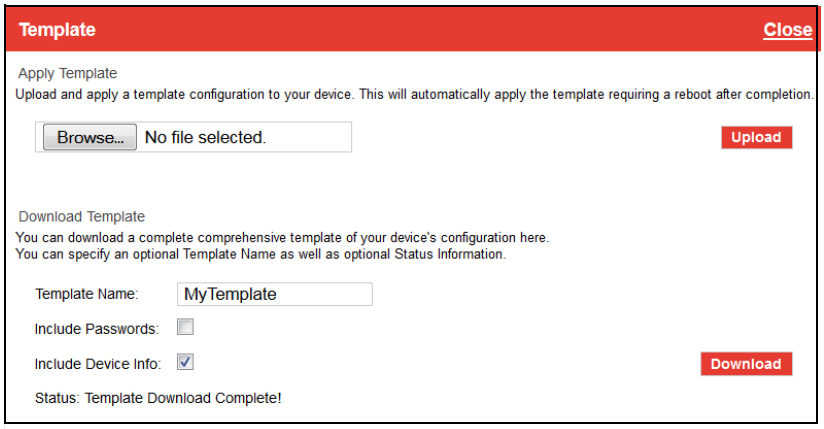

Template
Close
Apply Template
Upload and apply a template configuration to your device. This will automatically apply the template requiring a reboot after completion.
Browse...
No file selected.
Upload
Download Template
You can download a complete comprehensive template of your device's configuration here.
You can specify an optional Template Name as well as optional Status Information.
Template Name:
MyTemplate
Include Passwords:
Include Device Info:
Download
Status: Template Download Complete!

Figure 2-5: Download template complete

Once the download is complete, the following window opens:

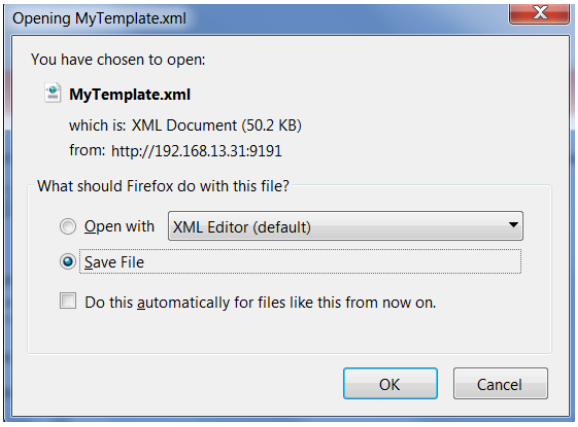


Figure 2-6: Open or Save the template file

6. In most cases, you will want to save the file to your computer for uploading to other AirLink devices, but you also have the option to open the file.
   - Select Save File and click OK—file is saved to your computer (by default to the Downloads folder). If you entered a template name, the file is saved using that name. Otherwise, it is saved under the default name, SWIApplyTemplate.xml.

- Select Open and click OK—file opens in a text or XML editor as a human readable file. Use this option if you selected Include Device Info when you saved the file and want to view the device information (the text between the <devicestatus> and </devicestatus> tags is the snap-shot of the Device Info), or you want to compare this template with another template.

Warning: *Do not attempt to change settings directly in the template file. Changing settings in the template file could result in unexpected behavior in the AirLink device. Alter the template only if you are specifically directed to do so by your distributor or Sierra Wireless Technical Support.*

Tip: *If you want to compare a new template with the previous one, download and save the old template before applying the new one. You can use any 3rd party text comparison tool to check the differences between two templates.*

Applying a Template

Note: If you are using Internet Explorer 9 to upload the template, see Templates on page 469 for instructions on configuring the browser's Internet options to allow the upload.

To upload and apply a template to an AirLink device:

1. Connect the computer (where the template is saved) to the AirLink device you want to upload the template to.
2. In ACEmanager, click the Template button on the toolbar.

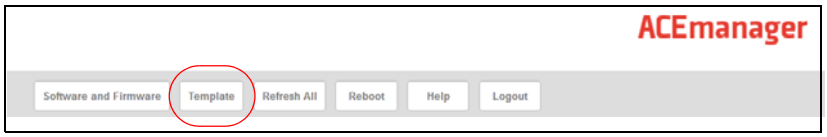


Figure 2-7: ACEmanager: Template button

The following window appears:

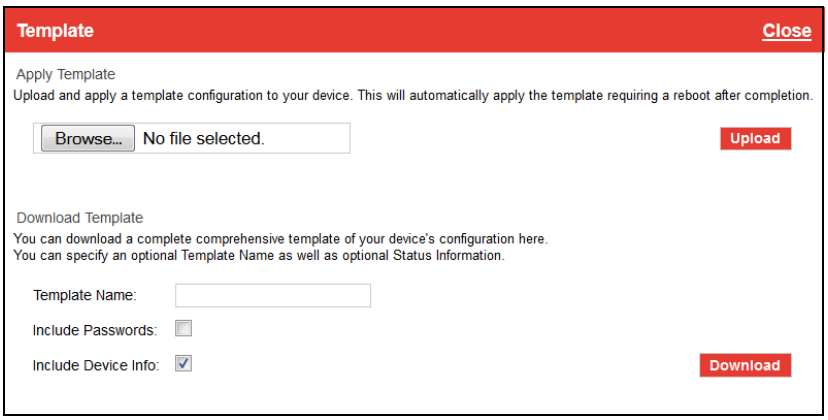

Template
Close
Apply Template
Upload and apply a template configuration to your device. This will automatically apply the template requiring a reboot after completion.
Browse...
No file selected.
Upload
Download Template
You can download a complete comprehensive template of your device's configuration here.
You can specify an optional Template Name as well as optional Status Information.
Template Name:
Include Passwords:
Include Device Info:
Download

Figure 2-8: ACEmanager: Template window

Use the top half of the window to upload and apply a template to your AirLink device.

3. Click Browse... and navigate to the template you want to upload.
4. Click Open. The template file name appears beside the Browse... button.

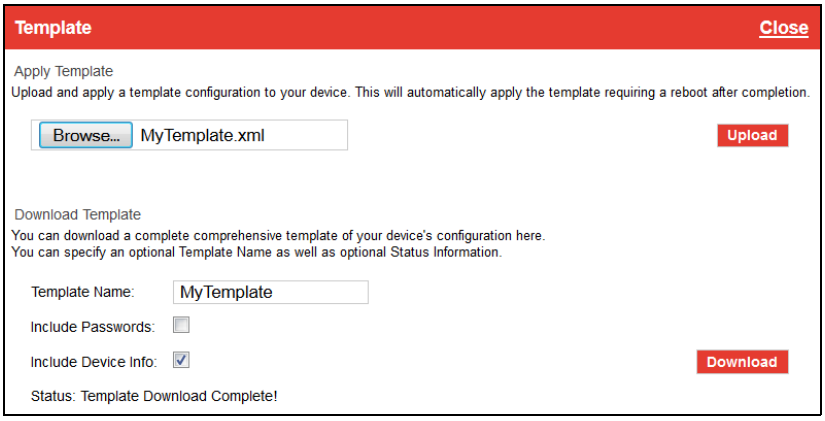

Template
Close
Apply Template
Upload and apply a template configuration to your device. This will automatically apply the template requiring a reboot after completion.
Browse...
MyTemplate.xml
Upload
Download Template
You can download a complete comprehensive template of your device's configuration here.
You can specify an optional Template Name as well as optional Status Information.
Template Name:
MyTemplate
Include Passwords:
Include Device Info:
Download
Status: Template Download Complete!

Figure 2-9: Apply Template file opened

5. Click Upload.
6. When the upload is complete, a Reboot button appears on the window.

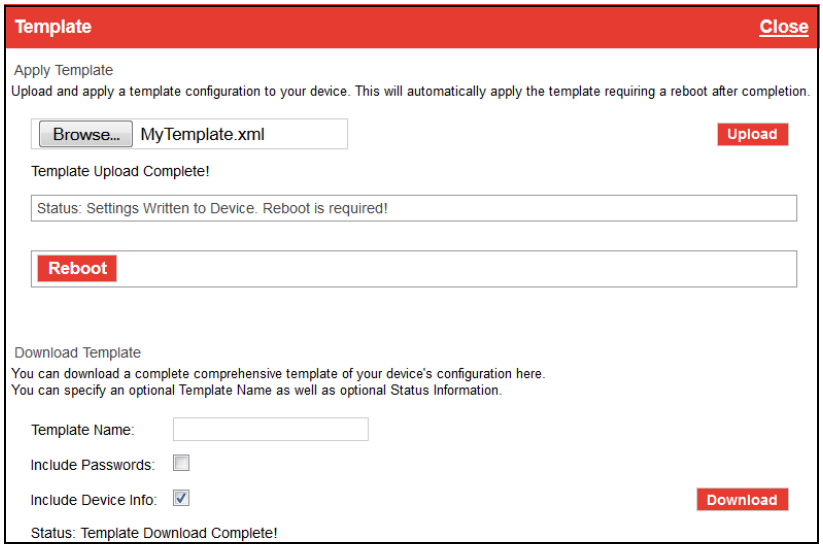

Template
Close
Apply Template
Upload and apply a template configuration to your device. This will automatically apply the template requiring a reboot after completion.
Browse...
MyTemplate.xml
Upload
Template Upload Complete!
Status: Settings Written to Device. Reboot is required!
Reboot
Download Template
You can download a complete comprehensive template of your device's configuration here.
You can specify an optional Template Name as well as optional Status Information.
Template Name:
Include Passwords:
Include Device Info:
Download
Status: Template Download Complete!

Figure 2-10: Template file uploaded

7. Click Reboot.
8. To confirm that the new template has been applied or to find out which template is currently on a device, go to Status > About and check the Template Name field.

Note: The Template Name field shows the last template applied and does not indicate any configuration changes made since the last template was applied.

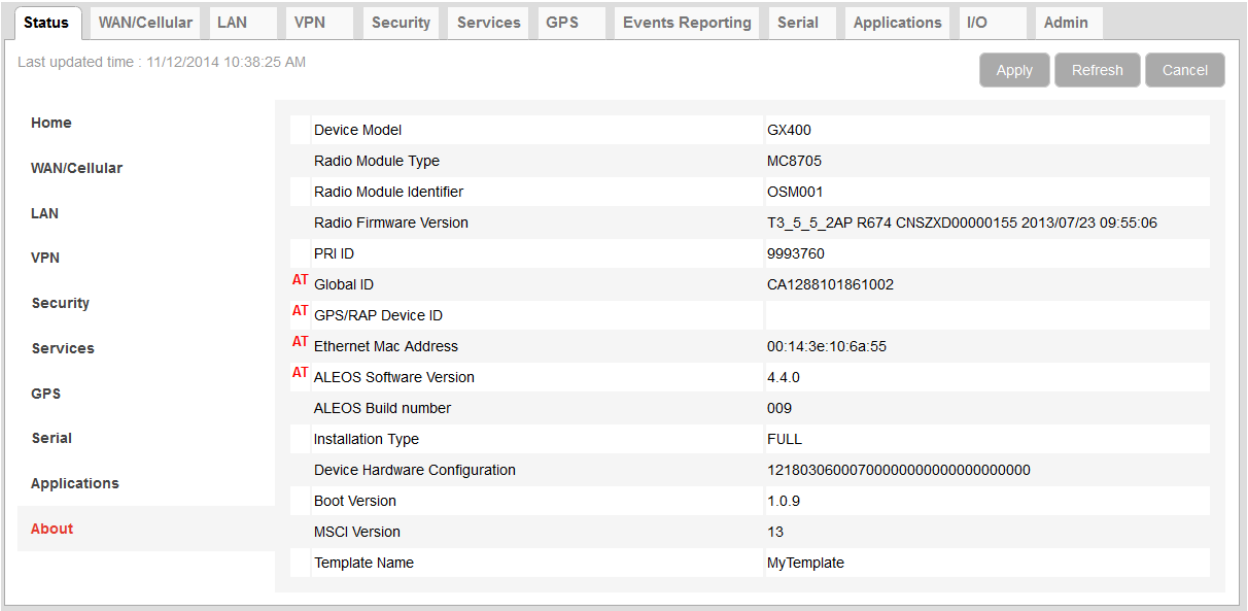


Figure 2-11: ACEmanager: Status > About

Note: If no template has been applied to the device since it was set or reset to the factory default settings, the template field is blank.

SSH PAD Mode

SSH PAD mode allows a PAD mode TCP connection to be encrypted using an SSH tunnel and a serial connection to the router or other connected device.

Figure 2-12 shows the network configuration.

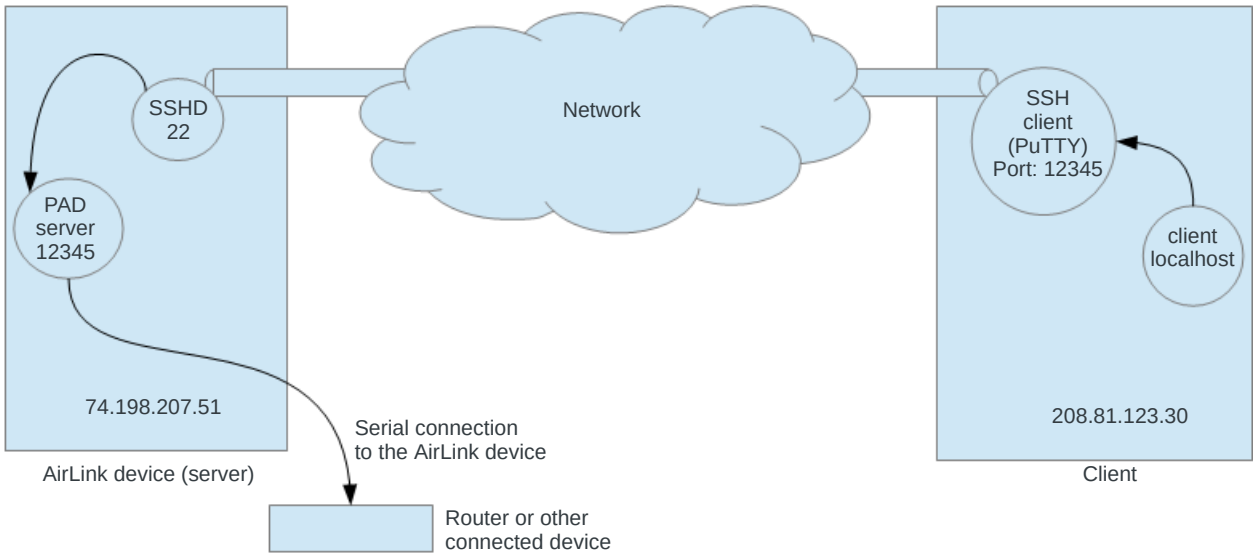


Figure 2-12: SSH Network

Note: For the purpose of illustration, this user guide uses port 12345 on the client, the default port 22 for creating an SSH section, and PuTTY as the SSH client throughout. When configuring SSH PAD mode, you can use any SSH client and values that are appropriate for your network.

The main steps in establishing a secure connection are:

1. Configure an SSH tunnel (on port 12345 in this example) on the client using an SSH client such as PuTTY.
2. Using the SSH client configuration to create the tunnel, log into the AirLink device with the user name and password. The SSH server authenticates the user.
3. The client application that wants to communicate with the PAD server on the AirLink device connects to “localhost” on port 12345.
4. Any data sent on this connection is tagged with a destination port of 12345.
5. The data is received by the SSH server on the AirLink device.
6. The SSH server receives the data with the tag of 12345 and uses port forwarding to send the data to the PAD server.

Server Configuration

You can enable SSH PAD mode on ALEOS by using functionality in the Secure Shell Daemon (SSHD) and by making some changes to the ACEmanager configuration. Currently, tunneled connections can only be initiated by a client that connects to the server on ALEOS.

Enabling SSH

The SSH Daemon must be running on the AirLink device. To enable it:

1. In ACEmanager, go to Services > Telnet/SSH, and in the Remote Login Server Mode drop-down menu, select SSH.
2. In the Remote Login Server Telnet/SSH Port field, enter the desired port number (or use the default SSH port 22).

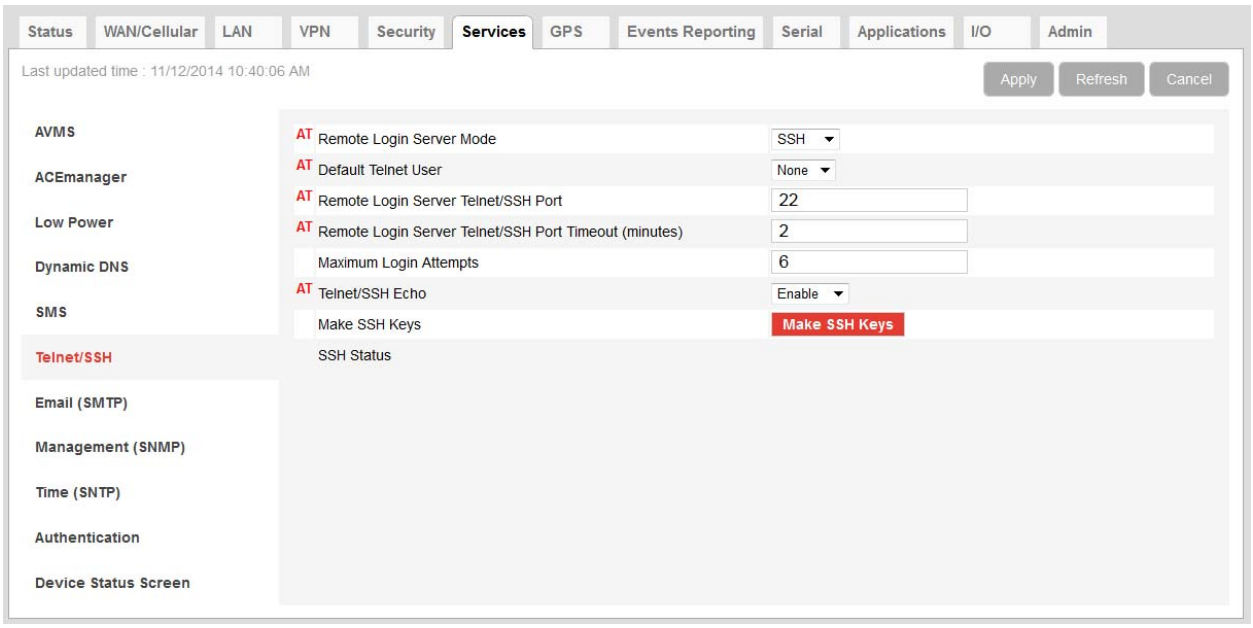


Figure 2-13: ACEmanager: Services > Telnet/SSH

3. Click Apply.

Enabling PAD Mode

ALEOS uses PAD mode to accept TCP connections. To enable PAD mode:

1. In ACEmanager, go to Serial > Port Configuration.
2. Set DB9 Serial Echo to Disable.
3. Set the Device Port field to the desired value (12345 in this example).
4. Set the destination Address to the IP address of the client that will be connecting to the AirLink device in SSH PAD mode.
5. Under Advanced, set Quiet Mode to Enable.
6. Under TCP, set TCP Auto Answer to Enable.

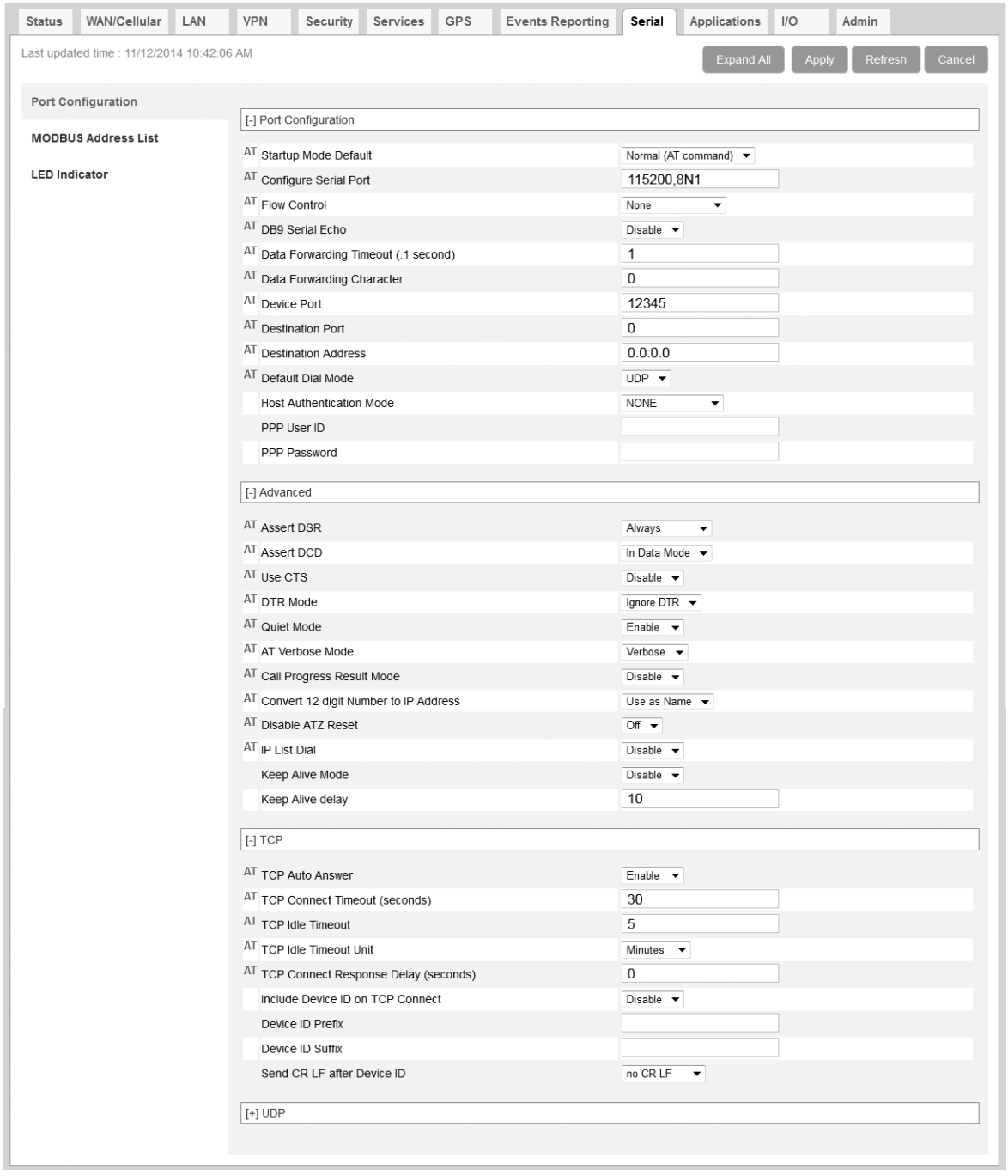


Figure 2-14: ACEmanager: Serial > Port Configuration

7. Click Apply.

Client Configuration

Creating Client Tunnel

Configure the SSH client to create a tunnel when it connects to the AirLink device. (In this example, PuTTY is used to create the tunnel.)

1. Create a new SSH session by entering the IP address of the AirLink device, and the configured port. (In this example, the IP Address of the AirLink device is 74.198.207.51 and default port 22 is used.)

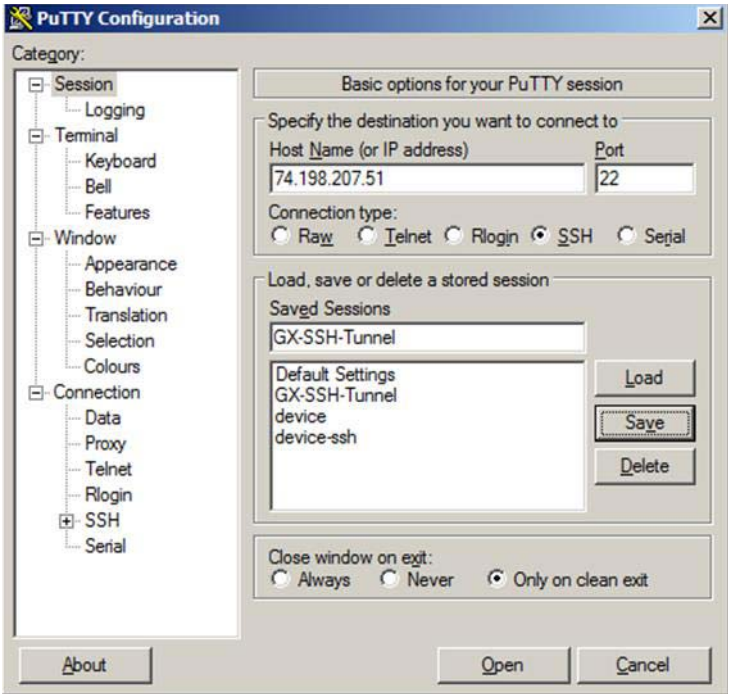


Figure 2-15: PuTTY: Creating a new SSH session

2. Click Save.
3. Go to Connection > SSH > Tunnels.
4. Create an SSH tunnel for the connection by creating a forwarded port.

   In the Source port field, enter the same value as the Device Port field configured in ACEmanager Serial port configuration (12345 in this example). This is the port that the PAD session listens on for incoming connections.

   In the Destination address field, enter the IP address of the AirLink device. (You can find this in ACEmanager on the Status > Home page.) The port is also listening to the TCP port for PAD mode (Device Port on the Serial tab) which, in this example, is 12345.

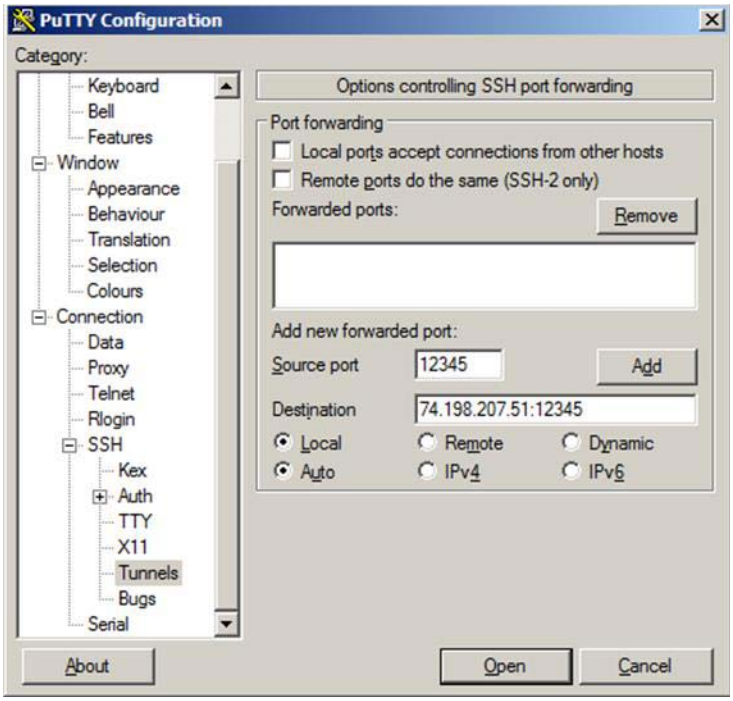


Figure 2-16: PuTTY: Creating an SSH tunnel

5. Leave the Local and Auto settings selected.

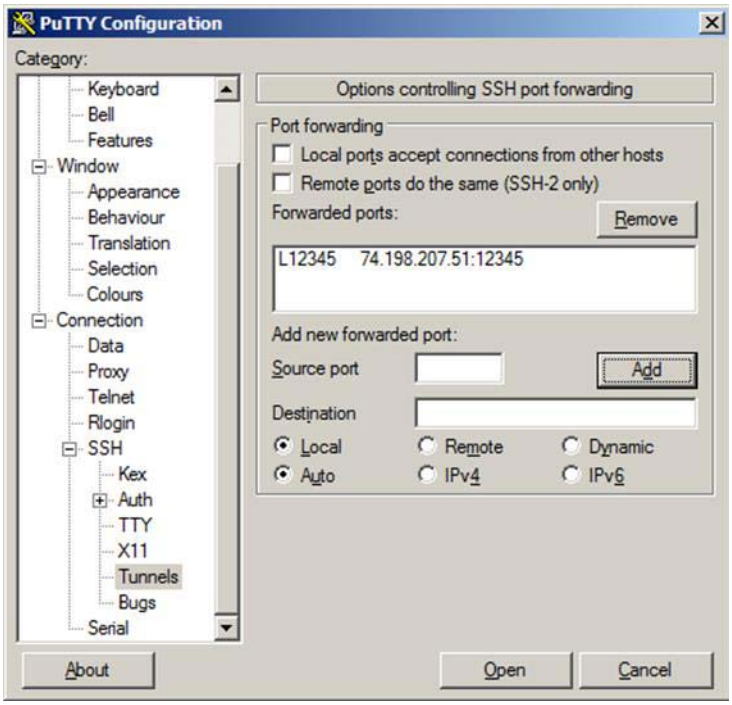


Figure 2-17: PuTTY: SSH tunnel created

6. Click Add.
7. Go to Connection > SSH.

8. Under Protocol options, select “Don’t start a shell or command at all” to prevent getting a command prompt.

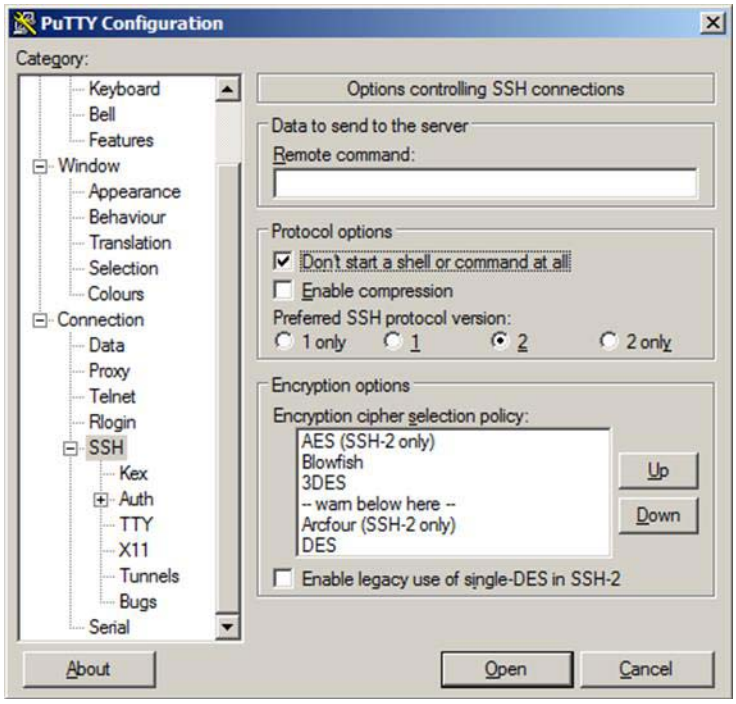


Figure 2-18: PuTTY: SSH Connection Settings

9. Click Open to create a connection to the AirLink device. Log in with the user account.
10. With the client application, establish a TCP connection to localhost using the configured port. (In this example, 12345.)

Important: *If you connect to the IP address of the AirLink device (74.198.207.51) instead of localhost, the tunnel is bypassed and the data is unencrypted.*

All data transmitted to the AirLink device should now be encrypted.

Update the ALEOS Software and Radio Module Firmware

To take advantage of new features available in the latest version of ALEOS, update the ALEOS software and radio module firmware on your AirLink devices.

You can use ACEmanager to update one device at a time or AVMS to update one or multiple devices at the same time.

Step 1—Planning Your Update

Note: These instructions are for upgrading from ALEOS 4.3.6 to 4.4.0. If you have an older version of ALEOS, refer to the Application Note: Updating from Older Versions of ALEOS.

1. For each of the devices you want to update, make a note of the:
   - Device Model
   - Radio Module Type
   - Certified Mobile Network Operator
   - ALEOS Software Version

   This information is available in AVMS and in ACEmanager (Status > About).

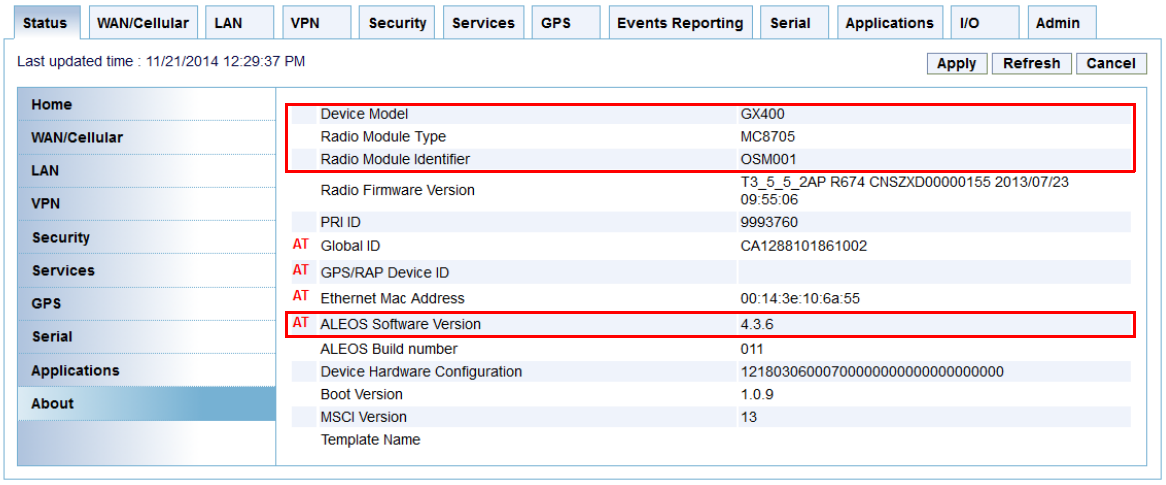


Figure 2-19: ACEmanager: Status > About

2. If you are planning to use ACEmanager to do the update:
   a. Go to www.sierrawireless.com/Support/Downloads.aspx and select your product and mobile network operator to get to the download page for your device.
   b. Download the new ALEOS software version for your system. If new radio module firmware is available, it is included with the ALEOS software in a .zip file. Do not install radio module firmware unless you are prompted to do so.

Note: If low power mode (see page 186) or time of day reset (page 327) are configured, and the following events are likely to coincide with the update:

- *The device entering low power mode*
- *The Time of Day reset occurring*

Sierra Wireless recommends that you disable these features before beginning the update.

Recommendations

If you have any questions about the update process, contact your authorized Sierra Wireless distributor before updating the radio module firmware.

Scheduling the update

The update can take up to 30 minutes to complete, depending on the speed of your network connection. The AirLink device being updated will be off-line during the update, so take this into account when scheduling the update.

Important: *BE PATIENT! The firmware update can take up to 30 minutes to complete. Ignore connection time out messages—the update process is still running.*

Waiting for the process to complete is faster than troubleshooting the problems that can be caused by interrupting the process midway. (Interrupting the process may result in having to return the device to the factory for repairs.)

Step 2—Update the ALEOS Software and Radio Module Firmware

Using ACEmanager to Update a Single AirLink Device

To update the ALEOS software and radio module firmware on one AirLink device:

1. Connect the AirLink device you want to update to your laptop, launch your browser and enter the URL for the device. The default IP address/port for the Ethernet interface is http://192.168.13.31:9191. If it is a remote device, enter the domain name or public IP (WAN) address.

Note: If you are connected to the device remotely, any files transferred to the device are transferred over-the-air and you may incur data charges.

2. Log in to ACEmanager.
   User name: user
   Default password: 12345
3. Go to Status > About and confirm that the current ALEOS version is 4.3.6. If not, see the note on page 30.
4. Click the Software and Firmware link.
   The Software and Firmware update window opens.

Note: These instructions show typical Software and Firmware update windows. Details such as the ALEOS version, device model, radio firmware version, etc. may vary, depending on the device you are updating.

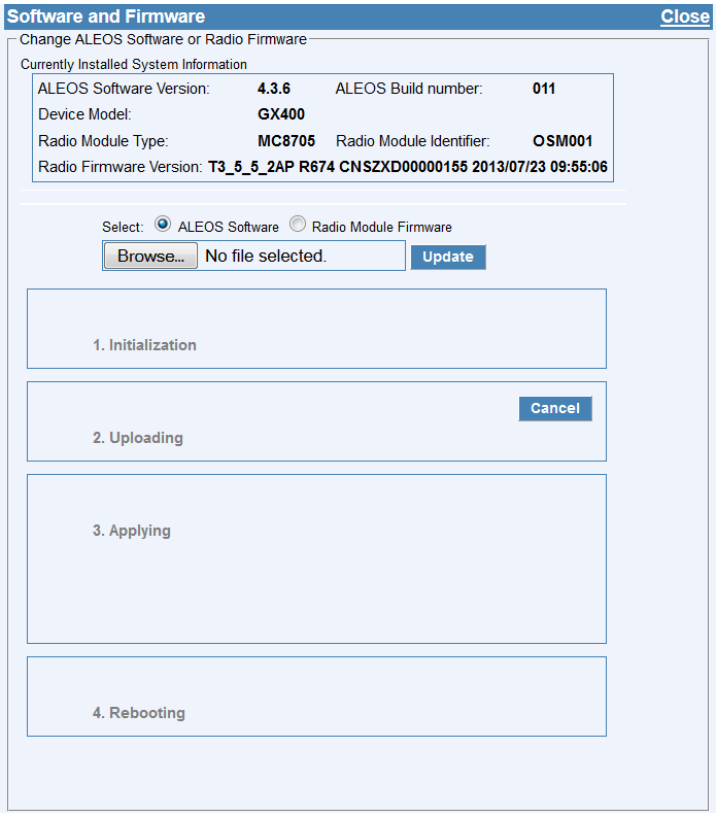


Figure 2-20: Software and Firmware update window

The update window gives you the option to update both ALEOS and the radio module firmware, or update only the radio module firmware. Unless advised otherwise by Sierra Wireless, we recommend that you select ALEOS software (which updates ALEOS and prompts you to update the radio module firmware if a newer version is available for your device).

5. Click Browse... and navigate to the ALEOS software you downloaded from the Sierra Wireless Web site.

Note: If you are updating only the radio module firmware, see Updating Only the Radio Module Firmware on page 36.

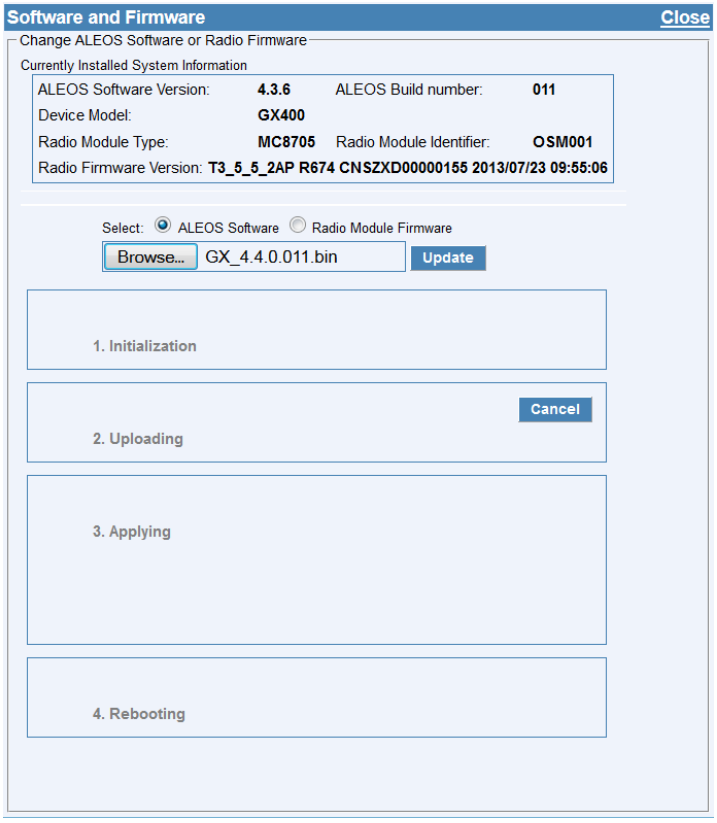


Figure 2-21: ALEOS file selected in Software and Firmware update window

6. Click Update.

   The ALEOS software update runs automatically and green check marks appear beside each step as it is completed.

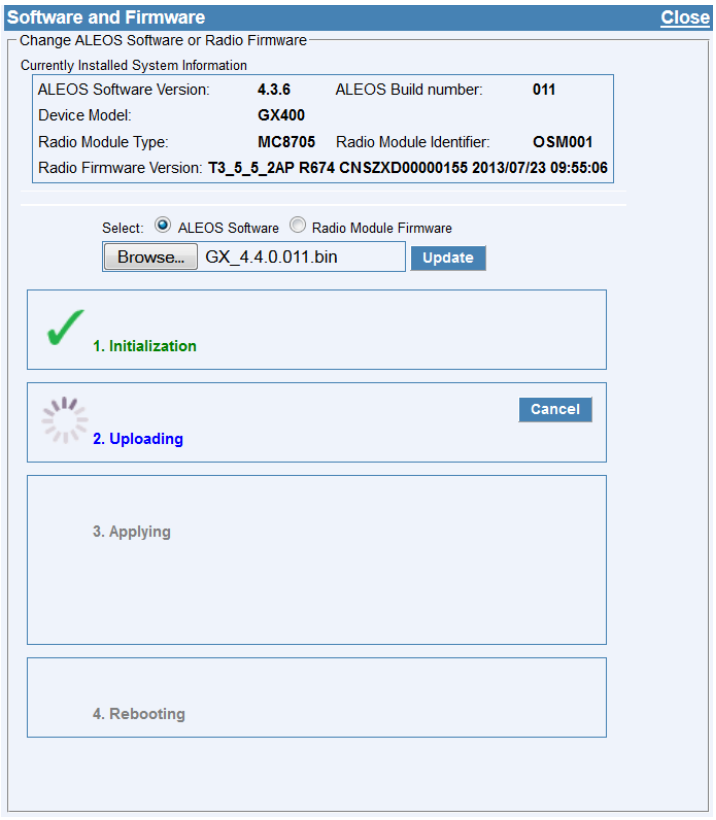


Figure 2-22: ALEOS software update in progress

Important: *Do not disconnect the AirLink device from the computer, and do not power cycle or reset the device during the update. If you see any error messages, refer to the* *Updating the ALEOS Software and Radio Module Firmware on page 457.*

7. Depending on the device and your Mobile Network Operator, You may be prompted to update the radio module firmware.

   If you do not receive a prompt, the radio firmware is up to date. Proceed to step 11.

   If you are prompted to update the firmware, proceed to step 8.

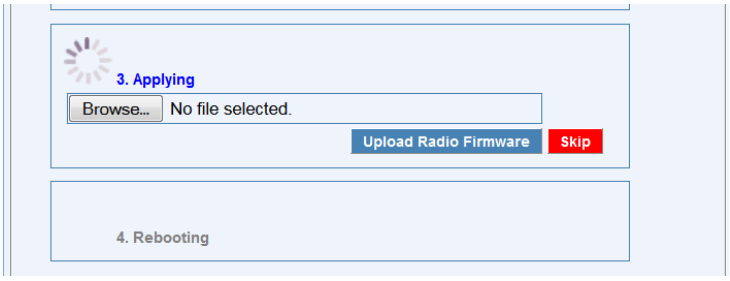


Figure 2-23: Prompt for Radio Module Firmware

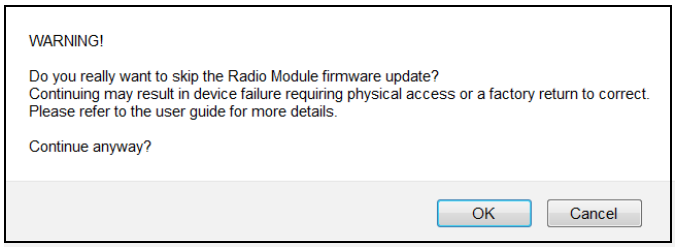
8. Under Applying, click Browse... and navigate to the radio module firmware file that was included in the .zip file you downloaded.
9. Click Open.

The firmware file name appears beside the Browse button.

10. Click Upload Radio Firmware.

    A message appears on the window indicating that the firmware has been successfully uploaded.

Note: Sierra Wireless recommends that you do NOT skip the radio module firmware update unless advised to do so by Sierra Wireless or an authorized distributor. If you choose to skip the radio module firmware update, you'll see the following warning.


WARNING!
Do you really want to skip the Radio Module firmware update?
Continuing may result in device failure requiring physical access or a factory return to correct.
Please refer to the user guide for more details.
Continue anyway?
OK
Cancel

Once the radio module firmware is uploaded, it begins applying the firmware upgrade. On the AirLink device, the LED chase begins to indicate that the firmware is being applied.

As indicated on the window, the radio module firmware may take 10 to 20 minutes to upload and install.

Important: *Do not disconnect the AirLink device from the computer or reboot the device while the firmware update is in progress. During the radio module firmware update, the device LEDs flash rapidly in sequence (an LED chase or caterpillar). When the radio module firmware update is complete, the device reboots automatically.*

If you see a message saying that the connection has timed out, ignore the message and continue to wait for the device to reboot.

If you clicked OK when you saw the timed out message and logged back in, you'll see the old version of the firmware. The firmware update process is still going on, so DO NOT reset the device or disconnect the power. DO NOT click Cancel. Continue to wait the 10 to 20 minutes for the radio module firmware update to complete. The device reboots once the firmware update is complete.

11. When the update is complete, the AirLink device reboots and you are returned to the Login screen.
12. When you see the Login screen, wait a few moments to ensure that the reboot is complete (or if you can see the device, check the LEDs) and then log in.
13. Go to Status > About.
14. Click Refresh.
15. Check the ALEOS Software Version and the Radio Firmware Version fields to confirm that the ALEOS software and the radio module firmware have been updated.

Using AirVantage Management Service (AVMS) to Update One or Multiple AirLink Devices Over-the-Air

You can use AirVantage Management Service to update the ALEOS software and radio module firmware over-the-air on one or multiple AirLink devices.

If you don't have an AVMS account:

1. In ACEmanager, go to the Services tab and ensure that AVMS is enabled and the server URL is http://na.m2mop.net/msci/com. If this is not the case, enter the correct URL, click Apply and then click Reboot.
2. Go to www.sierrawireless.com/en/productsandservices/AirVantage_M2M_-Cloud/Management_Service.aspx for more information. To sign up for a free trial account, go to http://na.airvantage.net.

Updating to ALEOS software with an AVMS account:

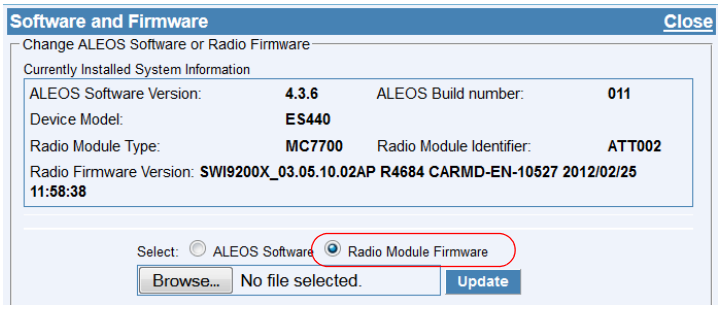
1. Go to http://na.airvantage.net/start and log in.
2. Follow the instructions in the online AVMS documentation to update the ALEOS software and radio module firmware.

Updating Only the Radio Module Firmware

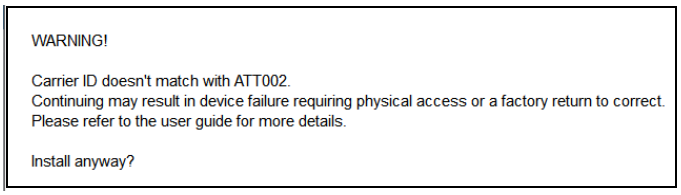
Note: Sierra Wireless recommends that you do NOT update only the radio module firmware unless advised to do so by Sierra Wireless or an authorized distributor.

If you are updating only the Radio Module Firmware:

1. Select the Radio Module Firmware button



2. Select the appropriate firmware file for your device and click Update. If you select a file for radio module firmware that is not supported on your device, you will see a warning message similar to the following:


WARNING!
Carrier ID doesn't match with ATT002.
Continuing may result in device failure requiring physical access or a factory return to correct.
Please refer to the user guide for more details.
Install anyway?

   Unless you have been advised by Sierra Wireless to do so, we recommend that you do not install an unsupported version of the radio module firmware.

3. Click Update.

The radio module firmware update runs automatically and green check marks appear beside each step as it is completed.

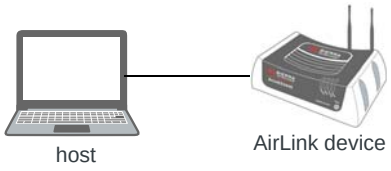
4. When the update is complete, the AirLink device reboots and you are returned to the Login screen.
5. When you see the Login screen, wait a few moments to ensure that the reboot is complete (or if you can see the device, check the LEDs) and then log in.
6. Go to Status > About.
7. Check the Radio Firmware Version has been updated.

Enterprise LAN Management

You can use AirLink devices in the following configurations:

- Standalone with a connection to a single host

  When using the AirLink device with a single host, ensure that the host is DHCP enabled.



- With a router

  The router allows several hosts to use the AirLink device's connection to the network. When using the AirLink device with a router:

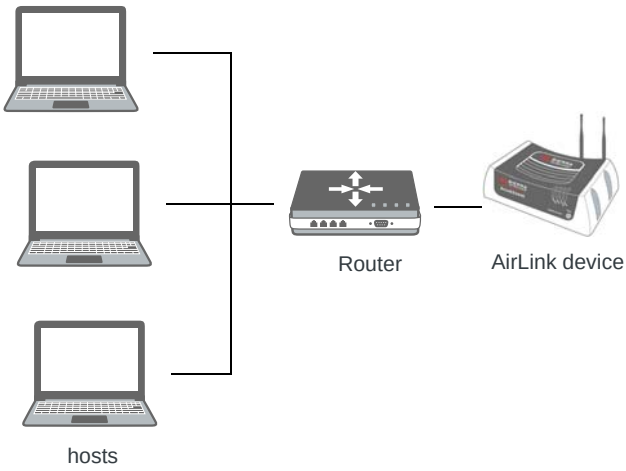
  - Configure the router to be DHCP enabled.

  And either:

  - Configure the router to use Network Address Translation (NAT).

    Or

  - Configure ALEOS (in ACEmanager) to use Host Port Routing. For information on using ALEOS with a router that is not configured to use NAT, see Host Port Routing on page 128.



Note: Other than for VLANs, ALEOS does not provide DHCP addresses to router connected hosts.

Over the Air (OTA) Connections

Access AirLink devices

You can use an OTA connection to access AirLink devices that are in either configuration described above (stand alone or with a router).

Access connected hosts

To use an OTA connection to access a connected host through the AirLink device, configure the host in ALEOS as the DMZ or port forwarding destination. For information on inbound OTA connections to the host, see DMZ on page 173 and Port Forwarding on page 169.

Configuring Your Device for use in a PCI Compliant System

The credit card industry requires retailers to comply with Payment Card Industry (PCI) standard to maintain a secure environment when processing payment card transactions. For these transactions, the AirLink device acts as a wireless data conduit for routers and PoSs (point-of-sale-terminals) that have been configured for PCI compliance.

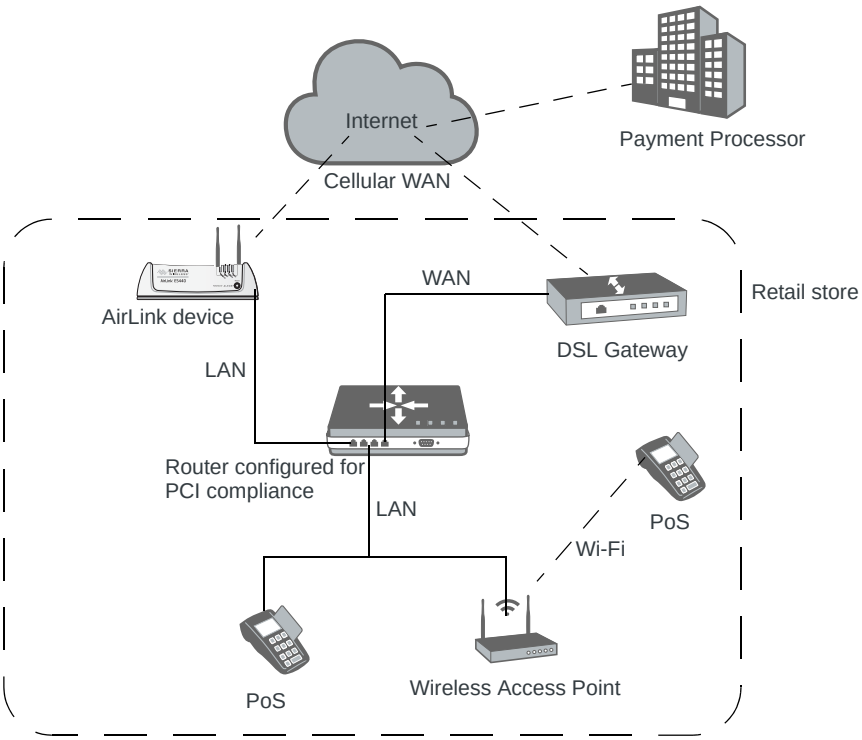


Figure 2-24: Sample PCI compliant network

The PCI compliant network must be set up so that:

- The USBnet is on a different subnet from the point-of-sale-terminal.
- All security protocols must be established from the point-of-sale terminal to the payment processor.
- Payment card terminals must be on a dedicated LAN or VLAN.
- The AirLink device must be connected to a router that is configured for PCI compliance.

Note: The serial port on the AirLink device has no access to the IP data path and does not need to be disabled.

If you are using the AirLink device for a payment card industry application, to meet PCI Data Security Standard compliance requirements the following steps must be done by a PCI certified service company.

For each device:

1. Connect the AirLink device to a router that has been configured for PCI compliance.
2. Log in to ACEmanager. (User name is user; default password is 12345.)
   Change the password regularly, in accordance with PCI recommendations.
3. Go to the Admin tab and change the default password.
   Do not share the ACEmanager password.
4. Go to Applications > ALEOS Application Framework and set the ALEOS Application Framework field to Disable.

3: Status

All of the fields in the Status group are read-only and provide information about the AirLink device. Depending on the individual settings and the onboard cellular module of the AirLink device, the actual status pages may look different than the screen shots shown here. The individual status sections give an accurate view of the current running configuration of the AirLink device. Refer to the following sections for information about the individual configuration options.

Tip: *To be sure you are viewing the current status for all fields, it's a good idea to first click the Refresh button on the upper right side of the screen.*

Home

The Home section of the Status tab is the first page displayed when you login to ACEmanager. It shows basic information about the cellular network connection and important information about the device.

Tip: *See WAN/Cellular Configuration on page 75 for information about configuring the cellular settings.*

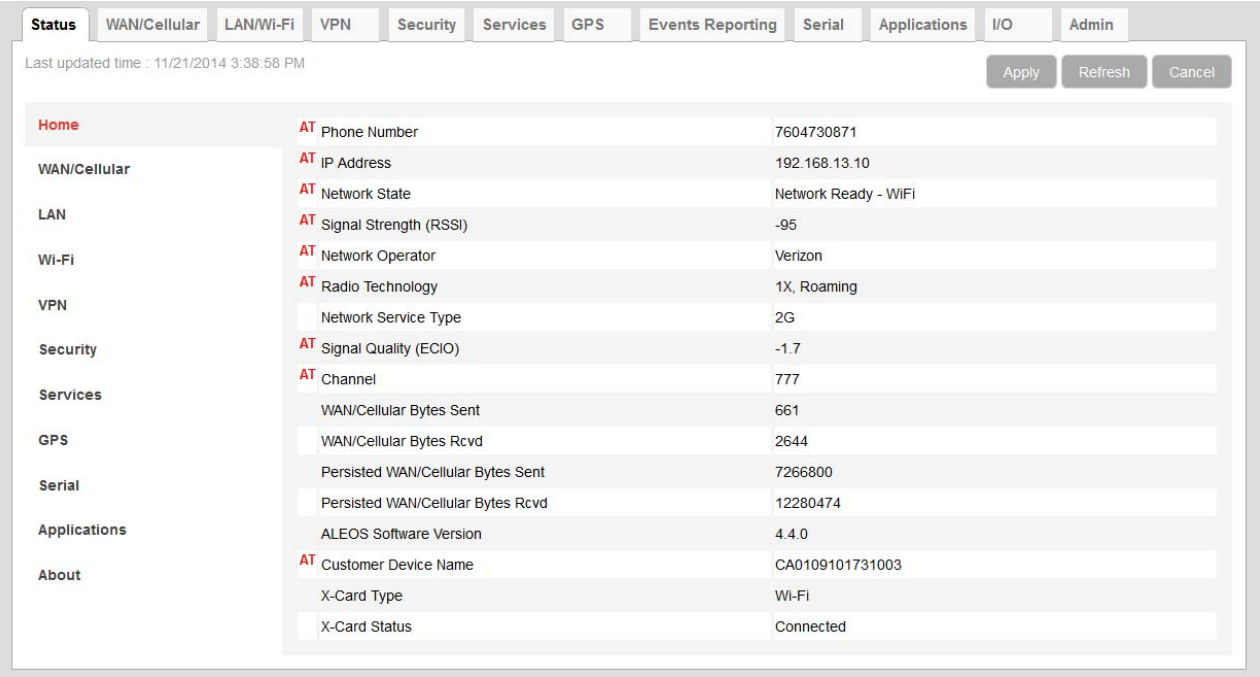


Figure 3-1: ACEmanager: Status > Home — CDMA (Radio Modules MC5728 and SL5011)

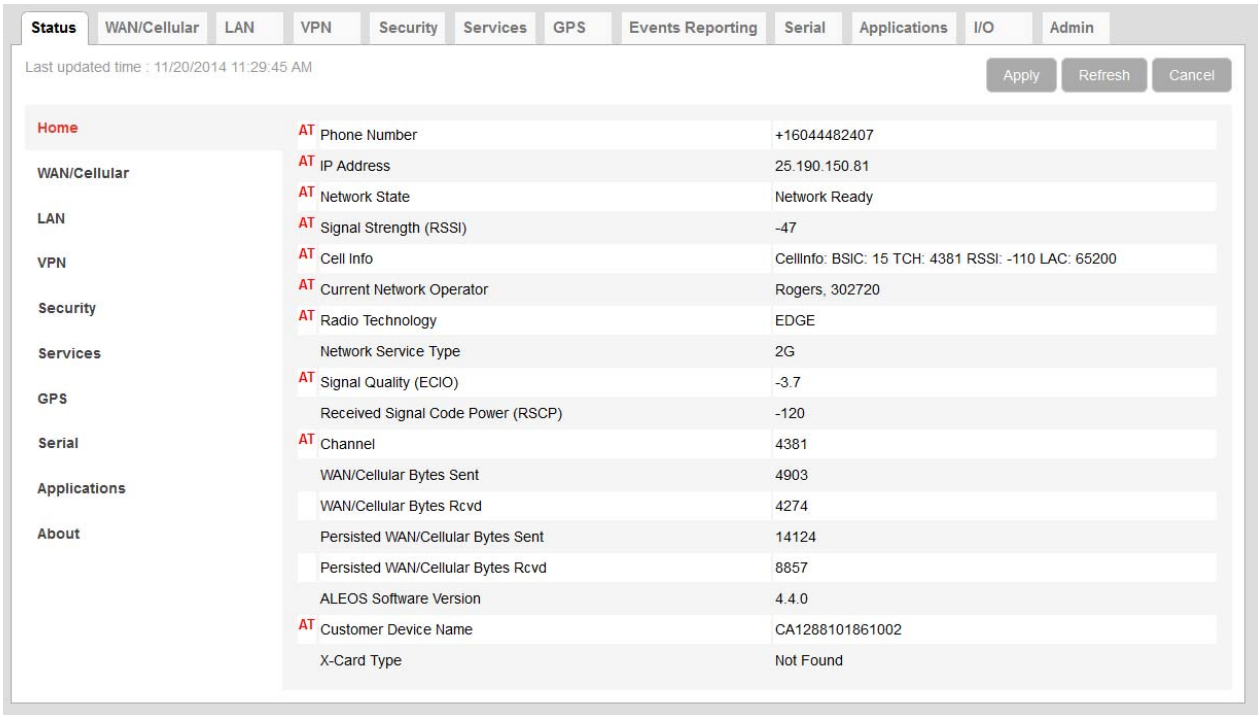


Figure 3-2: ACEmanager: Status > Home — HSPA (Radio Modules MC8705, SL8090, and SL8092)

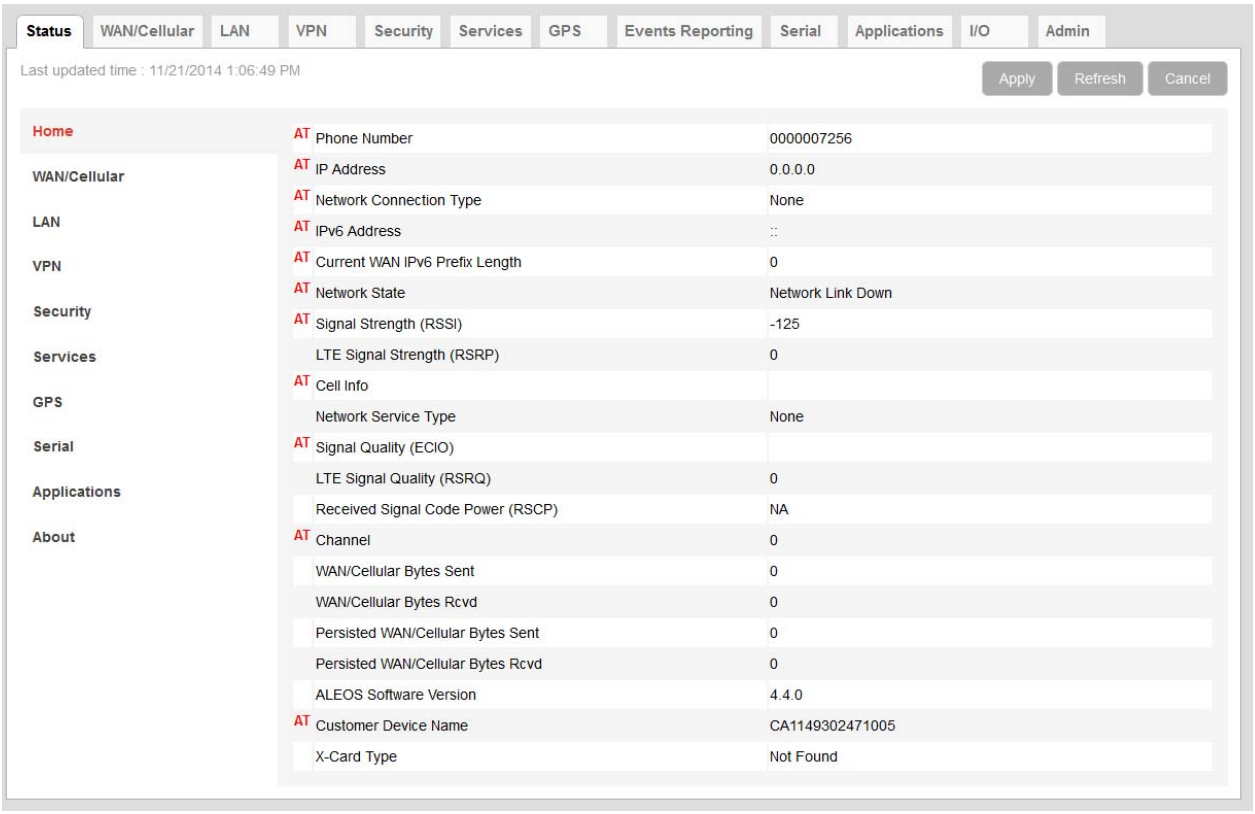


Figure 3-3: ACEmanager: Status > Home — LTE (Radio Module MC7750)

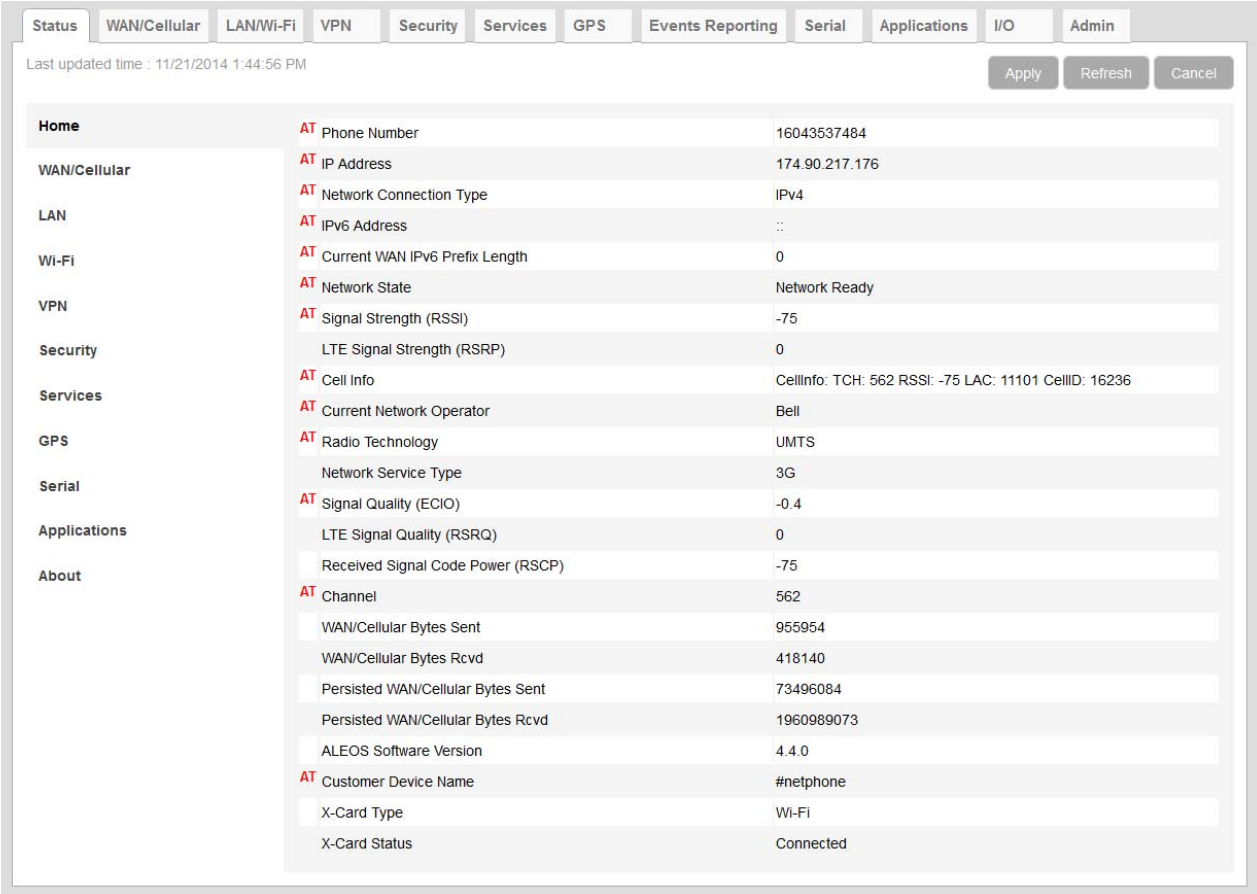


Figure 3-4: ACEmanager: Status > Home — LTE (Radio Module MC7710 and MC7700)

Field	Description
Phone Number	The phone number (programmed into the device) associated with the Mobile Network Operator account. If the Mobile Network Operator does not allow the account to display the phone number, a “dummy” phone number is displayed.
IP Address	The current IPv4 WAN IP address for the device. When Wi-Fi client mode is active, the IP address used by Wi-Fi is shown. For more information, see Client (Wi-Fi WAN) Mode on page 134.
Network Connection Type	This field is GX440-specific and only appears if the IP Address Preference field on the WAN/ Cellular tab is set to IPv4 and IPv6 Gateway. Displays the type of IP connection that has been established (None, IPv4, or Both IPv4 and IPv6)
IPv6 Address	This field is GX440-specific and only appears if the IP Address Preference field on the WAN/ Cellular tab is set to IPv4 and IPv6 Gateway. If you have an IPv6 connection, this field displays the IP address. If not, it displays “::” (two colons).

Current WAN IPv6 Prefix Length	This field is GX440-specific and only appears if the IP Address Preference field on the WAN/Cellular tab is set to IPv4 and IPv6 Gateway. Displays the length (number of bits) of the IPv6 Address Network Prefix.
Network State	Current state of the cellular radio network connection • Network Ready—Connected to a mobile broadband network and ready to transfer data • Network Ready Wi-Fi—Connected to a Wi-Fi network and ready to transfer data • Connecting To Network—Establishing a network connection; wait until the connection is established • Connecting To Network - Wi-Fi—Establishing a connection to a Wi-Fi network; wait until the connection is established • Not Connected-Wait for Activity—The Always on connection field on the WAN/Cellular tab (Advanced section) is set to Disabled. The device connects to the cellular network only when it needs to send or receive data. • Data connection failed. Waiting to retry—ALEOS is attempting to reconnect to the mobile broadband network. Ensure that the APN is correct or the account is activated to the ESN for your device. Wait until it is able to connect. If you see this status repeatedly or for an extended period of time, contact your Mobile Network Operator. • Network Link Down—Unable to connect to the network. Ensure that the APN is correct or the account is activated to the ESN for your device. If the problem persists, contact your Mobile Network Operator. • Network Link Down - Wi-Fi—Unable to connect to the Wi-Fi access point. Check the authentication information. • No SIM or Unexpected SIM Status—Unable to read the SIM information; check that the SIM card is installed correctly. • SIM PIN incorrect x attempts left—Wrong SIM PIN entered; enter the correct PIN. If the correct PIN is not entered in the specified number of attempts, the SIM is blocked. Contact your Mobile Network Operator to unblock the SIM. • No Service—Unable to connect to the broadband network. Check that the antenna is connected properly. If the problem persists, contact your Mobile Network Operator for information about coverage in your region. • Provisioning...—(CDMA networks only) The Mobile Network Operator is updating the radio module firmware with your account details. Wait until the provisioning is complete. • Awaiting provisioning...—(CDMA networks only) The device does not yet have an account associated with the radio module and is attempting to contact the Mobile Network Operator to obtain account information. If this state persists, check that the account is activated to the device's ESN. • Starting OMADM state—The Mobile Network Operator is starting an over-the-air (OTA) radio module device management session. Wait until the OTA management session is complete. • In NI PRL Update—(CDMA networks only) An updated Preferred Roaming List is being downloaded from the network. Wait until the download is complete. • NI PRL Failed—(CDMA networks only) The network initiated attempt to update the Preferred Roaming List failed. If the problem persists, contact your Mobile Network Operator. • NI PRL Failed. Waiting to retry—(CDMA networks only) The network initiated attempt to update the Preferred Roaming List failed. The network is waiting to retry the download. Wait until the download is complete. • Network Authentication Failed—Unable to connect to the network because of invalid authentication data. If the problem persists, contact your Mobile Network Operator.

<table>
<tr><td>Signal Strength (RSSI)</td><td>Received Signal Strength Indicator
The average received signal power measured in the air interface channel
Indicates if there is a strong signal available for the AirLink device to connect to
See also LTE Signal Strength (RSRP) and LTE Signal Quality (RSRQ).
The value varies, depending on the network characteristics and the AirLink device.
<table><tr><th>RSSI</th><th>Signal strength</th></tr><tr><td>> -70 dBm</td><td>Excellent</td></tr><tr><td>-70 dBm to -85 dBm</td><td>Good</td></tr><tr><td>-86 dBm to -100 dBm</td><td>Fair</td></tr><tr><td>< -100 dBm</td><td>Poor</td></tr><tr><td>-110 dBm</td><td>No signal</td></tr></table></td></tr>
<tr><td>LTE Signal Strength (RSRP)</td><td>Reference Signal Received Power
The average signal power of all cell-specific reference signals within the LTE channel
Indicates whether the AirLink device has a strong connection to the wireless network
The value varies, depending on the network characteristics and the AirLink device.
<table><tr><th>RSRP</th><th>Signal strength</th></tr><tr><td>> -90 dBm</td><td>Excellent</td></tr><tr><td>-90 dBm to -105 dBm</td><td>Good</td></tr><tr><td>-106 dBm to -120 dBm</td><td>Fair</td></tr><tr><td>< -120 dBm</td><td>Poor</td></tr></table>See also LTE Signal Quality (RSRQ) and Signal Strength (RSSI).</td></tr>
<tr><td>Cell Info</td><td>Cell information such as the Base Station Identity Code (BSIC), TCH, Received Signal Strength Indicator (RSSI), Location Area Code (LAC), and the cell ID
For additional information, including cell info for LTE networks, see *CELLINFO2? on page 389 and LTE Networks on page 463.</td></tr>
<tr><td>Current Network Operator</td><td>Name of the Mobile Network Operator whose network the AirLink device is connected to
Note: The roaming operator is only displayed if the home operator allows this.</td></tr>
<tr><td>Radio Technology</td><td>Type of service being used by the device (LTE, HSPA+, DC_HSPA+, 1xRTT, EV-DO, UMTS, HSPA, EDGE or GPRS)
If you are connected to a network other than that of your Mobile Network Operator, the network service type indicates that you are roaming (and additional charges may apply).</td></tr>
<tr><td>Network Service Type</td><td>Type of network the device is connected to (4G, 3G, 2G)</td></tr>
</table>

<table>
<tr><td>Signal Quality (EC/IO)</td><td>CDMA/UMTS signal quality
Indicates the signal quality with a ratio of the average signal energy to co-channel interference in dB
<table><tr><th>EC/IO</th><th>Signal quality</th></tr><tr><td>0 to -6</td><td>Excellent</td></tr><tr><td>-7 to -10</td><td>Good</td></tr><tr><td>-11 to -20</td><td>Fair to Poor</td></tr></table></td></tr>
<tr><td>LTE Signal Quality (RSRQ)</td><td>Reference Signal Received Quality
The RSRQ indicates the quality of the AirLink device’s connection to the wireless network. (Is noise or interference affecting the quality of the connection?) See also Signal Strength (RSSI) and LTE Signal Strength (RSRP).
The value varies, depending on the network characteristics and the AirLink device.
<table><tr><th>RSRQ</th><th>Signal quality</th></tr><tr><td>> -9 dB</td><td>Excellent</td></tr><tr><td>-9 dB to -12 dB</td><td>Good</td></tr><tr><td>< -13 dB</td><td>Fair to Poor</td></tr></table>
Note: For additional information on the LTE network, use the *CELLINFO2? AT command (described on page 389).</td></tr>
<tr><td>Received Signal Code Power (RSCP)</td><td>The RSCP is the power measured by the receiver on a particular physical channel. It provides an indication of signal strength for UMTS connections. Expected values are in the range of -50 dB to -120 dB.</td></tr>
<tr><td>Channel</td><td>CDMA/UMTS channel
The current active channel number for the cellular network connection</td></tr>
<tr><td>WAN/Cellular Bytes Sent</td><td>Number of bytes sent to the network since system startup or reboot</td></tr>
<tr><td>WAN/Cellular Bytes Rcvd</td><td>Number of bytes received from the network since system startup</td></tr>
<tr><td>Persisted WAN/ Cellular Bytes Sent</td><td>Number of bytes sent
The count starts when device first goes on air and persists over reboot. The field resets to zero on reset to factory default settings.</td></tr>
<tr><td>Persisted WAN/ Cellular Bytes Rcvd</td><td>Number of bytes received
The count starts when device first goes on air and persists over reboot. The field resets to zero on reset to factory default settings.</td></tr>
<tr><td>ALEOS Software Version</td><td>Version of ALEOS software currently installed in the device</td></tr>
</table>

X-Card Type	Indicates whether the AirLink device has a connected X-Card or not Values are: • Not Found • Wi-Fi • Dual Ethernet • IO *Note: This field applies only to the AirLink GX Series devices.*
X-Card Status	Indicates the status of the X-Card, if present Values are: • Connected • Disconnected *Note: This field applies only to the AirLink GX Series devices.*

WAN/Cellular

WAN/Cellular provides specific information about the cellular connection including IP address and how much data has been transmitted or received. Some of the information on this page is repeated on the Home page for quick reference.

EV-DO/CDMA

This section applies to devices with radio module MC5728 and SL5011.

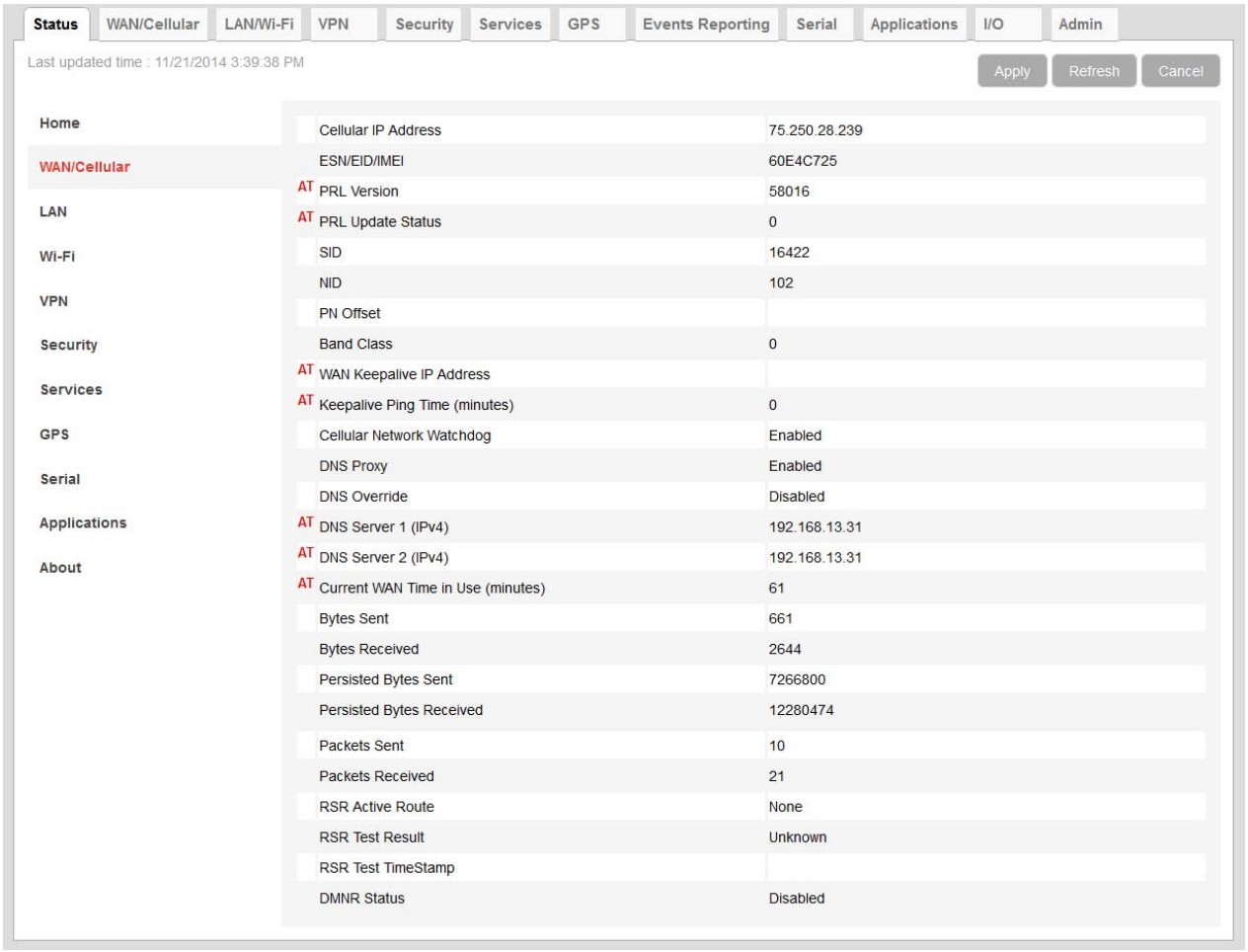


Figure 3-5: ACEmanager: Status > WAN/Cellular — CDMA

Field	Description
Cellular IP Address	Current IP address assigned by the Mobile Network Operator.
ESN/EID/IMEI	Electronic Serial Number for the internal radio
PRL Version	Version of the Preferred Roaming List installed in the device

Field	Description
PRL Update Status	Status of the last PRL (Preferred Roaming List) update. 0 if there has been none
SID	System ID
NID	Network ID
PN Offset	Base station identifier used in CDMA networks
Band Class	CDMA band class
Keepalive IP Address	IP address that WAN Keep Alive uses to test cellular connectivity (if enabled)
WAN Keepalive Ping Time (minutes)	Amount of time between Keepalive pings in minutes
DNS Proxy	Determines which DNS server the connected clients use for domain name resolution • Enabled—DNS Proxy is activated. Connected clients acquire the AirLink device's IP address as their DNS server. The AirLink device performs DNS lookups on behalf of the clients. • Disabled—DNS Proxy is deactivated. If DNS Override is set to Enable, connected clients acquire the DNS servers defined by the Mobile Network Operator. If DNS override is set to Disable, connected clients acquire the DNS servers specified by the Alternate DNS settings. To set this option, see DNS Proxy on page 140.
DNS Override	Override WAN-granted DNS
DNS Server 1 (IPv4)	1st DNS server IP address currently in use by the Network connection to resolve domain names into IP addresses
DNS Server 2 (IPv4)	2nd DNS server IP address
Current WAN Time in Use (minutes)	The time in minutes from which the cellular IP is obtained from the mobile network *Note: The value of this field is 0 if the device is not connected to a cellular network.*
Bytes Sent	Number of bytes sent to the cellular network since system startup or reboot
Bytes Received	Number of bytes received from the cellular network since system startup or reboot
Persisted Bytes Sent	Number of bytes sent The count starts when device first goes on air and persists over reboot. The field resets to zero on reset to factory default settings.
Persisted Bytes Received	Number of bytes received The count starts when device first goes on air and persists over reboot. The field resets to zero on reset to factory default settings.
Packets Sent	Number of packets sent to the network since system startup or reboot
Packets Received	Number of packets received from the network since system startup or reboot

Field	Description
RSR Active Route	Active route for Reliable Static Routing • Primary—Specified network traffic is currently using the configured primary route. • Backup—Specified network traffic is currently using the configured backup route. • None—RSR is not enabled.
RSR Test Result	Result of the most recent Tracking Object test
RSR Test TimeStamp	Time of the most recent Tracking Object test
DMNR Status	Dynamic Mobile Network Routing (DMNR) status • Enabled • Disabled
DMNR Foreign Agent Registration Status	This field only appears when DMNR is enabled. The status of transactions with the Home agent • Pass—Connected subnets registered or de-registered successfully • Fail—Unable to register or de-register connected subnets • Unknown
DMNR Reverse Tunnelling Agent Status	This field only appears when DMNR is enabled. Status of the NEMO tunnel • Up • Down

GSM/HSPA

This section applies to devices with radio module MC8705, SL8090, and SL8092.

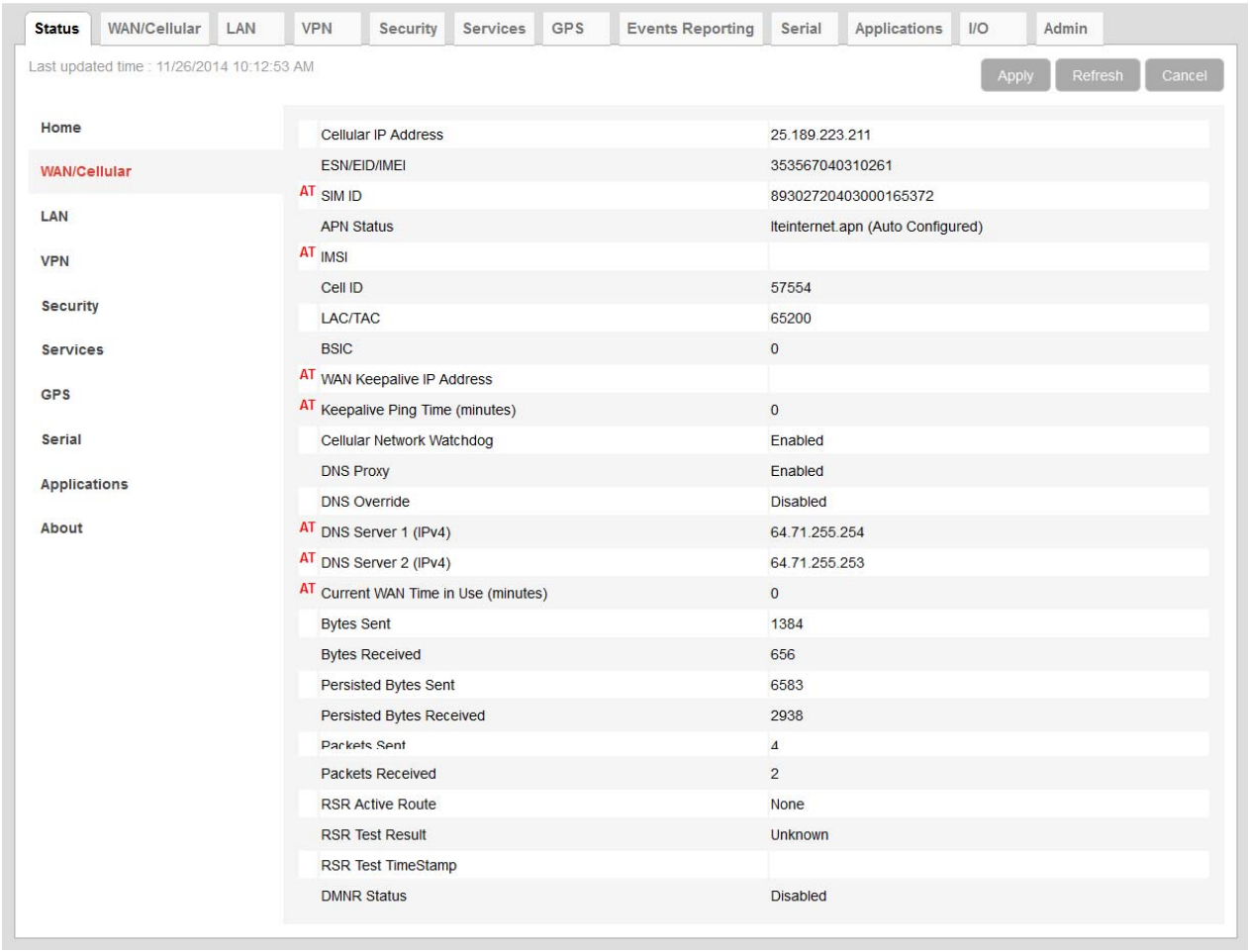


Figure 3-6: ACEmanager: Status > WAN/Cellular — GSM / HSPA

Field	Description
Cellular IP Address	Cellular IP Address
ESN/EID/IMEI	Electronic Serial Number for the internal radio
SIM ID	Identification number for the SIM card in use
APN Status	Current APN in use by the network connection • (Auto Configured) is a default APN based on the SIM card in use. • (User Entered) is a custom APN entered manually into the configuration. *Note: APN is configured on the WAN/Cellular configuration tab.*
IMSI	International Mobile Subscriber Identity number

Field	Description
Cell ID	Unique number that identifies each base transceiver station (BTS) or sector of a BTS within an LAC
LAC/TAC	Location Area Code or Tracking Area Code (LTE)
BSIC	Base Station Identity Code
WAN Keepalive IP Address	IP address that WAN Keep Alive uses to test cellular connectivity (if enabled)
Keepalive Ping Time (minutes)	Amount of time between Keepalive pings in minutes
Cellular Network Watchdog	Status of the Cellular Network Watchdog (Enabled or Disabled)
DNS Proxy	Determines which DNS server the connected clients use for domain name resolution • Enabled—DNS Proxy is activated. Connected clients acquire the AirLink device's IP address as their DNS server. The AirLink device performs DNS lookups on behalf of the clients. • Disabled—DNS Proxy is deactivated. If DNS Override is set to Enable, connected clients acquire the DNS servers defined by the Mobile Network Operator. If DNS Override is set to Disable, connected clients acquire the DNS servers specified by the Alternate DNS settings. To set this option, see DNS Proxy on page 140.
DNS Override	Override WAN-granted DNS
DNS Server 1	1st DNS server IP address currently in use by the Network connection to resolve domain names into IP addresses
DNS Server 2	2nd DNS server IP address
Current WAN Time in Use (Minutes)	The time in minutes from which the cellular IP is obtained from the mobile network *Note: The value of this field is 0 if the device is not connected to a cellular network.*
Bytes Sent	Number of bytes sent to the cellular network since system startup or reboot
Bytes Received	Number of bytes received from the network since system startup or reboot
Packets Sent	Number of packets sent to the network since system startup or reboot
Persisted Bytes Sent	Number of bytes sent The count starts when device first goes on air and persists over reboot. The field resets to zero on reset to factory default settings.
Persisted Bytes Received	Number of bytes received The count starts when device first goes on air and persists over reboot. The field resets to zero on reset to factory default settings.
Packets Received	Number of packets received from the network since system startup or reboot

Field	Description
RSR Active Route	Active route for Reliable Static Routing • Primary—Specified network traffic is currently using the configured primary route. • Backup—Specified network traffic is currently using the configured backup route. • None—RSR is not enabled.
RSR Test Result	Result of the most recent Object Tracking test
RSR Test TimeStamp	Time of the most recent Object Tracking test
DMNR Status	DMNR is only supported on the Verizon Wireless network.

LTE—Fallback to EV-DO

This section applies to devices with radio module MC7750.

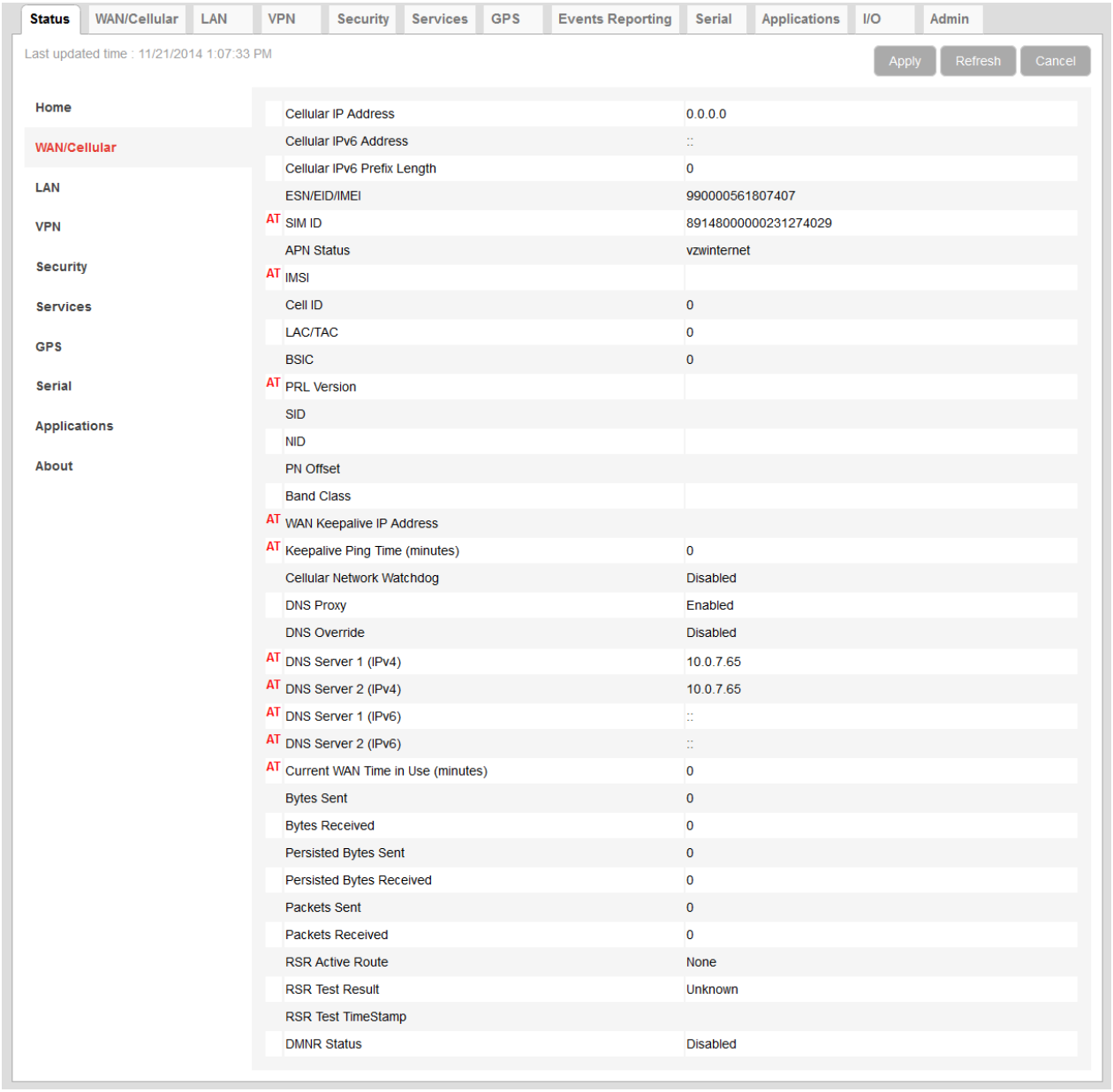


Figure 3-7: ACEmanager: Status > WAN/Cellular — LTE - Fallback to EV-DO

Field	Description
Cellular IP Address	Cellular IPv4 WAN IP Address
IPv6 is supported only on the AirLink GX440. For more information, see IP Address Preference on page 84.	

Field	Description
Cellular IPv6 Address	This field is GX440-specific and only appears if the IP Address Preference field on the WAN/Cellular tab is set to IPv4 and IPv6 Gateway. If you have an IPv6 connection, this field displays the IP address. If not, it displays "::" (two colons).
Cellular IPv6 Prefix Length	This field is GX440-specific and only appears if the IP Address Preference field on the WAN/Cellular tab is set to IPv4 and IPv6 Gateway. Displays the length (number of bits) of the IPv6 Address Network Prefix.
ESN/EID/IMEI	Electronic Serial Number for the internal radio
SIM ID	Identification number for the SIM card in use
APN Status	Current APN in use by the network connection • (Auto Configured) is a default APN based on the SIM card in use. • (User Entered) is a custom APN entered manually into the configuration. *Note: APN is configured on the WAN/Cellular configuration tab.*
IMSI	International Mobile Subscriber Identity number
Cell ID	Unique number that identifies each base transceiver station (BTS) or sector of a BTS within an LAC
LAC/TAC	Location Area Code or Tracking Area Code (LTE)
BSIC	Base Station Identity Code
PRL Version	Version of the Preferred Roaming List installed in the device
SID	System ID
NID	Network ID
PN Offset	Base station identifier used in CDMA networks
Band Class	Radio frequency (For detailed information see LTE Networks on page 463.)
WAN Keepalive IP Address	IP address that WAN Keep Alive uses to test cellular connectivity (if enabled)
Keepalive Ping Time (minutes)	Amount of time between Keepalive pings in minutes
Cellular Network Watchdog	Status of the Cellular Network Watchdog (Enabled or Disabled)
DNS Proxy	Determines which DNS server the connected clients use for domain name resolution • Enabled—DNS Proxy is activated. Connected clients acquire the AirLink device's IP address as their DNS server. The AirLink device performs DNS lookups on behalf of the clients. • Disabled—DNS Proxy is deactivated. If DNS Override is set to Enable, connected clients acquire the DNS servers defined by the Mobile Network Operator. If DNS Override is set to Disable, connected clients acquire the DNS servers specified by the Alternate DNS settings. To set this option, see DNS Proxy on page 140.
DNS Override	Override WAN-granted DNS

Field	Description
DNS Server 1 (IPv4)	1st DNS server IP address currently in use by the Network connection to resolve domain names into IP addresses
DNS Server 2 (IPv4)	2nd DNS server IP address
DNS Server 1 (IPv6) **DNS Server 1 (IPv6)**	These two fields are displayed only if you have an AirLink GX440, and an IPv6 connection. • DNS Server 1 (IPv6) is the 1st IPv6 DNS server IP address that is passed to LAN clients for their use. • DNS Server 2 (IPv6) is the 2nd IPv6 DNS server IP address that is passed to LAN clients for their use.
Current WAN Time in Use (minutes)	The time in minutes from which the cellular IP is obtained from the mobile network *Note: The value of this field is 0 if the device is not connected to a cellular network.*
Bytes Sent	Number of bytes sent to the cellular network since system startup or reboot
Bytes Received	Number of bytes received from the network since system startup or reboot
Persisted Bytes Sent	Number of bytes sent The count starts when device first goes on air and persists over reboot. The field resets to zero on reset to factory default settings.
Persisted Bytes Received	Number of bytes received The count starts when device first goes on air and persists over reboot. The field resets to zero on reset to factory default settings.
Packets Sent	Number of packets sent to the network since system startup or reboot
Packets Received	Number of packets received from the network since system startup or reboot
RSR Active Route	Active route for Reliable Static Routing • Primary—Specified network traffic is currently using the configured primary route. • Backup—Specified network traffic is currently using the configured backup route. • None—RSR is not enabled.
RSR Test Result	Result of the most recent Object Tracking test
RSR Test TimeStamp	Time of the most recent Object Tracking test
DMNR Status	Dynamic Mobile Network Routing (DMNR) status • Enabled • Disabled

Field	Description
DMNR Foreign Agent Registration Status	This field only appears when DMNR is enabled. The status of transactions with the Home agent • Pass—Connected subnets registered or de-registered successfully • Fail—Unable to register or de-register connected subnets • Unknown
DMNR Reverse Tunnelling Agent Status	This field only appears when DMNR is enabled. Status of the NEMO tunnel • Up • Down

LTE—Fallback to GSM/HSPA

This section applies to devices with radio module MC7700 and MC7710.

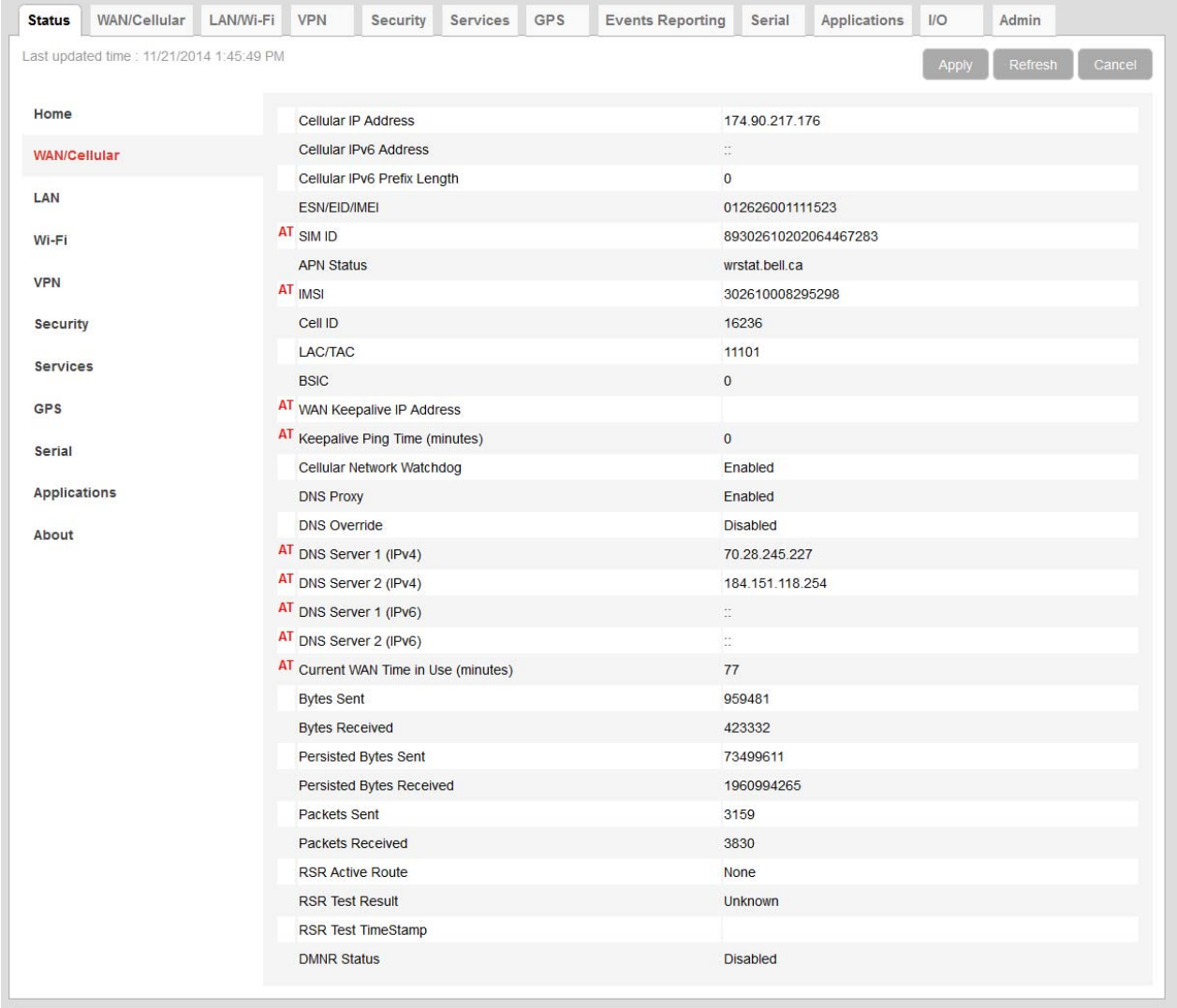


Figure 3-8: ACEmanager: Status > WAN/Cellular — LTE - Fallback to HSPA

Field	Description
Cellular IP Address	Cellular IPv4 WAN IP Address
IPv6 is supported only on the AirLink GX440. For more information, see IP Address Preference on page 84.	
Cellular IPv6 Address	This field is GX440-specific and only appears if the IP Address Preference field on the WAN/Cellular tab is set to IPv4 and IPv6 Gateway. If you have an IPv6 connection, this field displays the IP address. If not, it displays "::" (two colons).

Field	Description
Cellular IPv6 Prefix Length	This field is GX440-specific and only appears if the IP Address Preference field on the WAN/Cellular tab is set to IPv4 and IPv6 Gateway. Displays the length (number of bits) of the IPv6 Address Network Prefix.
ESN/EID/IMEI	Electronic Serial Number for the internal radio
SIM ID	Identification number for the SIM card in use
APN Status	Current APN in use by the network connection • (Auto Configured) is a default APN based on the SIM card in use. • (User Entered) is a custom APN entered manually into the configuration. *Note: APN is configured on the WAN/Cellular configuration tab.*
IMSI	International Mobile Subscriber Identity number
Cell ID	Unique number that identifies each base transceiver station (BTS) or sector of a BTS within an LAC
LAC/TAC	Location Area Code or Tracking Area Code (LTE)
BSIC	Base Station Identity Code
WAN Keepalive IP Address	IP address that WAN Keep Alive uses to test cellular connectivity (if enabled)
Keepalive Ping Time (minutes)	Amount of time between Keepalive pings in minutes
Cellular Network Watchdog	Status of the Cellular Network Watchdog (Enabled or Disabled)
DNS Proxy	Determines which DNS server the connected clients use for domain name resolution • Enable—DNS Proxy is activated. Connected clients acquire the AirLink device's IP address as their DNS server. The AirLink device performs DNS lookups on behalf of the clients. • Disable—DNS Proxy is deactivated. If DNS Override is set to Enable, connected clients acquire the DNS servers defined by the Mobile Network Operator. If DNS override is set to Disable, connected clients acquire the DNS servers specified by the Alternate DNS settings. To set this option, see DNS Proxy on page 140.
DNS Override	Override WAN-granted DNS
DNS Server 1 (IPv4)	1st DNS server IP address currently in use by the Network connection to resolve domain names into IP addresses
DNS Server 2 (IPv4)	2nd DNS server IP address
DNS Server 1 (IPv6) **DNS Server 2 (IPv6)**	These two fields are displayed only if you have an AirLink GX440, and an IPv6 connection. • DNS Server 1 (IPv6) is the 1st IPv6 DNS server IP address that is passed to LAN clients for their use. • DNS Server 2 (IPv6) is the 2nd IPv6 DNS server IP address that is passed to LAN clients for their use.

Field	Description
Current WAN Time in Use (minutes)	The time in minutes from which the cellular IP is obtained from the mobile network *Note: The value of this field is 0 if the device is not connected to a cellular network.*
Bytes Sent	Number of bytes sent to the cellular network since system startup or reboot
Bytes Received	Number of bytes received from the network since system startup or reboot
Persisted Bytes Sent	Number of bytes sent The count starts when device first goes on air and persists over reboot. The field resets to zero on reset to factory default settings.
Persisted Bytes Received	Number of bytes received The count starts when device first goes on air and persists over reboot. The field resets to zero on reset to factory default settings.
Packets Sent	Number of packets sent to the network since system startup or reboot
Packets Received	Number of packets received from the network since system startup or reboot
RSR Active Route	Active route for Reliable Static Routing • Primary—Specified network traffic is currently using the configured primary route. • Backup—Specified network traffic is currently using the configured backup route. • None—RSR is not enabled.
RSR Test Result	Result of the most recent Object Tracking test
RSR Test TimeStamp	Time of the most recent Object Tracking test
DMNR Status	DMNR is only supported on the Verizon Wireless network.

LAN

This is the status of the local network. It lists information about the network and connected clients.

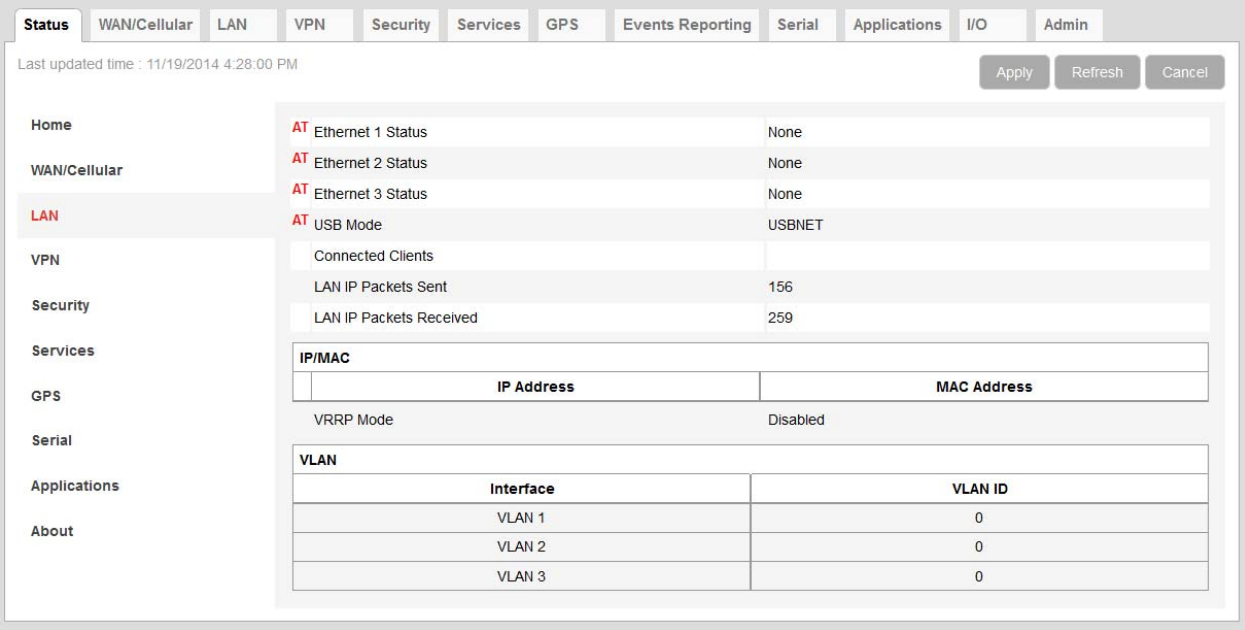


Figure 3-9: ACEmanager: Status > LAN (GX Series device with a Dual Ethernet X-Card installed)

Field	Description
Ethernet 1 Status	Speed and duplex status of the connection on Ethernet port 1 (the main Ethernet port). If there is no connection, the value is None.
Ethernet 2 Status	This field only appears on a GX Series device with a Dual Ethernet X-Card installed. Speed and duplex status of the connection on Ethernet port 2 on the Dual Ethernet X-Card. If there is no connection, the value is None.
Ethernet 3 Status	This field only appears on a GX Series device with a Dual Ethernet X-Card installed. Speed and duplex status of the connection on Ethernet port 3 on the Dual Ethernet X-Card. If there is no connection, the value is None.
USB Mode	Which USB port mode is set (USBnet, USB serial, or Disabled)
Connected Clients	Number of connected hosts that obtained their IP address through DHCP over Ethernet or USBnet. The value in this field does not include hosts connected via PPP or PPPoE.
LAN IP Packets Sent	Number of IP packets sent to the Ethernet host interface since the system startup *Note: If the AirLink GX Series device has a Dual Ethernet X-Card installed, the data reported includes all three Ethernet ports.*

Field	Description
LAN IP Packets Received	Number of IP packets received from the Ethernet host interface since the system startup *Note: If the AirLink GX Series device has a Dual Ethernet X-Card installed, the data reported includes all three Ethernet ports.*
IP/MAC table	Local IP Address and the MAC Address of connected hosts that obtain their IP address through DHCP. *Note: IPv6 clients are not shown.*
VRRP Enabled	Configuration of the VRRP feature
VLAN table	Identities (Interface name and ID) of the configured VLANs

Wi-Fi

If you have a GX Series device with a Wi-Fi X-Card installed, click the Wi-Fi tab on the left side of the screen to view the Wi-Fi status.

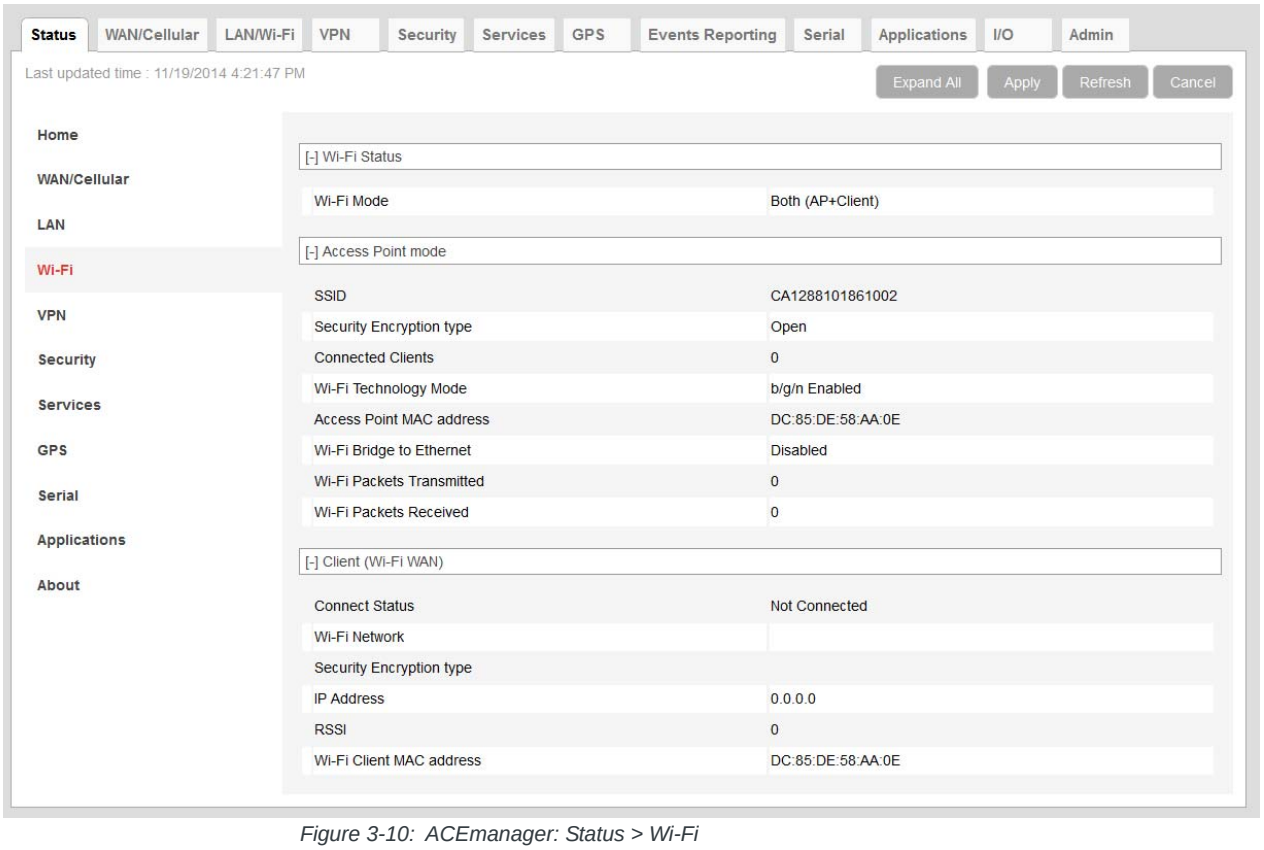


Figure 3-10: ACEmanager: Status > Wi-Fi

Field	Description
Wi-Fi Status	
Wi-Fi Mode	Wi-Fi mode. For more information, see Wi-Fi Mode on page 129.
Access Point mode	
SSID	Configured or default Wi-Fi SSID.
Security Encryption type	Wi-Fi security encryption (security authentication) type
Connected Clients	Number of connected clients
Wi-Fi Technology Mode	Wi-Fi Technology mode (b/g Enabled or b/g/n Enabled)
Access Point MAC address	MAC address hosts connect to when the GX Series device is configured as an access point. For more information, see Access Point Mode on page 130 and Both (AP + Client) Mode on page 138.
Wi-Fi Bridge to Ethernet	Status of the Bridge Wi-Fi to Ethernet field. When this feature is enabled, the Ethernet LAN hosts and the Wi-Fi access point hosts are on the same subnet. For details, see Bridge Wi-Fi to Ethernet on page 115.
Wi-Fi Packets Transmitted	Number of IP packets sent to the access point host interface over Wi-Fi since the system startup
Wi-Fi Packets Received	Number of IP packets received by the access point host interface over Wi-Fi since the system startup
Client mode	
Connect Status	Connection status
Wi-Fi Network	Wi-Fi network the AirLink device is connected to
Security Encryption type	Wi-Fi security encryption (security authentication) type
IP Address	WAN IP address the device received from the Access Point
RSSI	Signal strength (in dBm)
Wi-Fi Client MAC address	MAC address the GX Series device uses to connect to a Wi-Fi access point when it is configured for Client mode. For more information, see Client (Wi-Fi WAN) Mode on page 134 and Both (AP + Client) Mode on page 138.

VPN

The VPN section gives an overview of the VPN settings and indicates whether a VPN connection has been made.

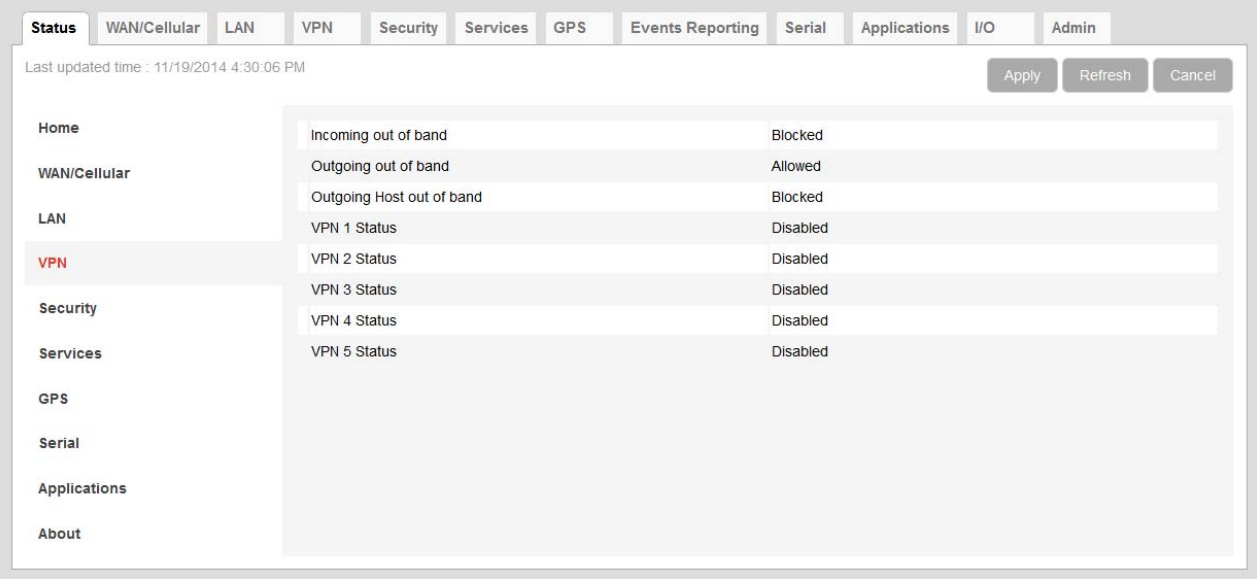


Figure 3-11: ACEmanager: Status > VPN

Field	Description
Incoming out of band	Whether incoming out of band traffic is allowed or blocked
Outgoing out of band	Whether outgoing ALEOS out of band traffic is allowed or blocked
Outgoing Host out of band	Whether Outgoing Host out of band traffic is allowed or blocked
VPN 1 to 5 Status	Status of each VPN connection: Disabled, Enabled, or Connected.

Security

The security section provides an overview of the security settings on the AirLink device.

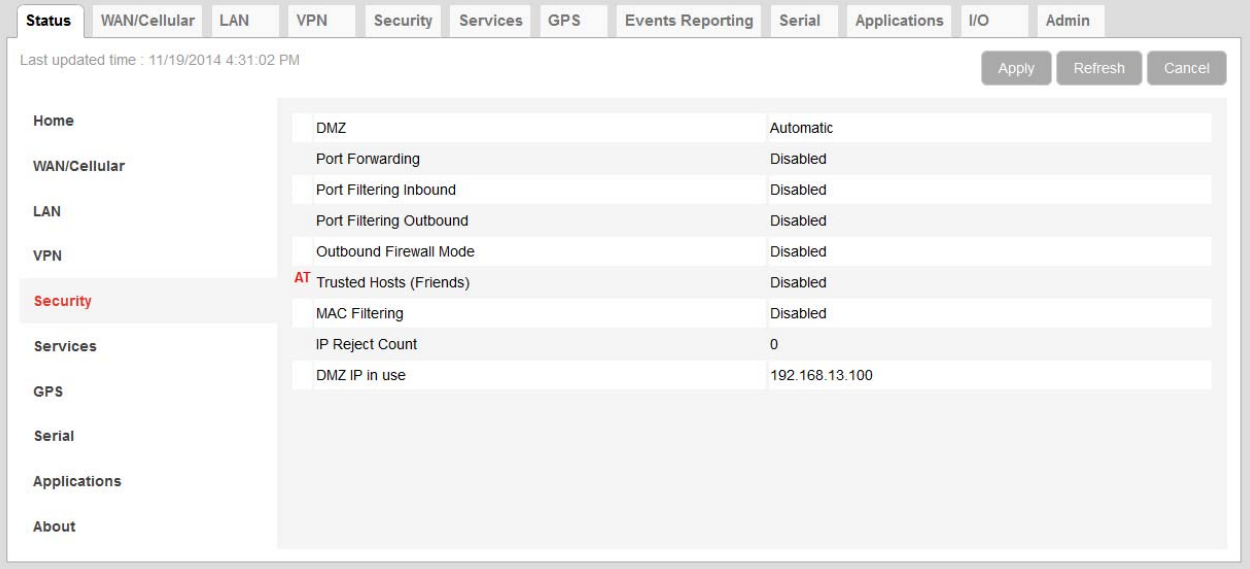


Figure 3-12: ACEmanager: Status > Security

Field	Description
DMZ	Status of DMZ (Automatic, Manual, or Disabled) DMZ defines a single LAN connected device where all unsolicited data should be routed.
Port Forwarding	Status of port forwarding (Enabled or Disabled)
Port Filtering Inbound	Status of inbound port filtering (Allowed Ports, Blocked Ports, or Not Used)
Port Filtering Outbound	Status of outbound port filtering (Allowed Ports, Blocked Ports, or Not Used)
Outbound Firewall Mode	Status of the outbound firewall (Enabled or Disabled)
Trusted Hosts (Friends)	Status of the Trusted Hosts (Friends) list (Disabled or Enabled) When this option is enabled, the AirLink device only accepts connections from trusted remote IP addresses.
MAC Filtering	Status of MAC filtering (Enabled or Disabled)
IP Reject Count	Number of IP addresses that have been rejected
DMZ IP in use	IP address currently in use for DMZ
Packet Inspection Level	Packet Inspection level (Normal or High)

Services

This section shows the status of AirLink services, including the ACEmanager access level.

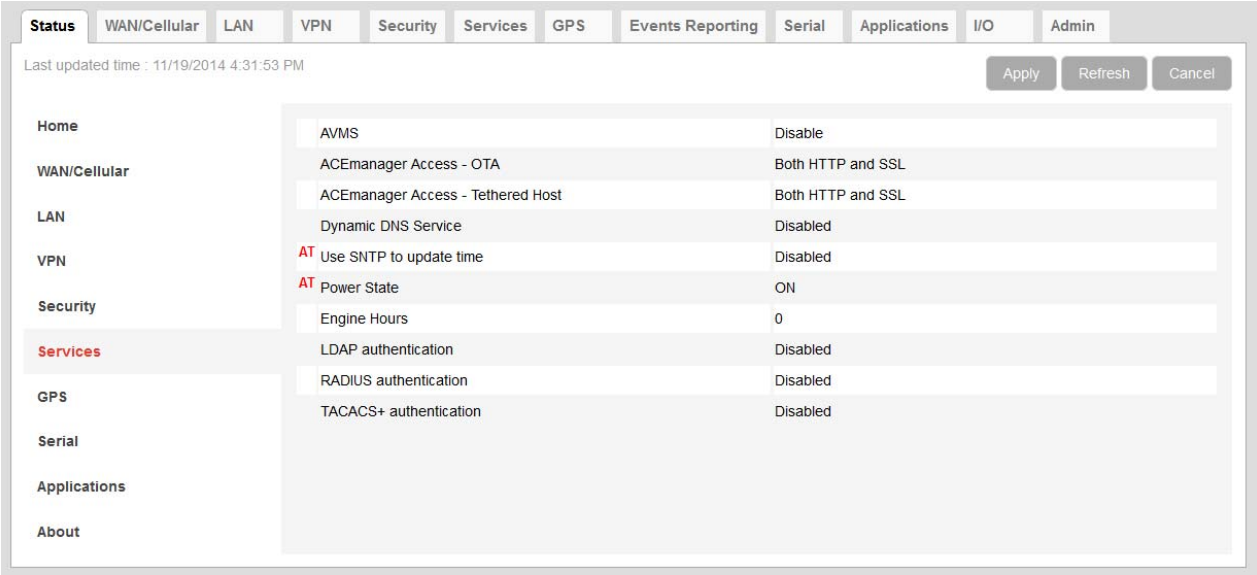


Figure 3-13: ACEmanager: Status > Services

Field	Description
AVMS	Status of the connection to the AirVantage Management Service
ACEmanager Access - OTA	ACEmanager over-the-air access mode (OFF, SSL Only, or Both HTTP and SSL [default])
ACEmanager Access - Tethered Host	ACEmanager access if tethered (physically connected) to Ethernet, USB, or RS232 (SSL Only or Both HTTP and SSL [default])
ACEmanager Access - Wi-Fi	ACEmanager Wi-Fi access (Same as host or Disabled)
Dynamic DNS Service	Service in use for Dynamic DNS translation
Full Domain Name	If the Dynamic DNS Service is configured to use a 3rd party host, the domain name configured is displayed. If the Dynamic DNS Service is configured to use IP Manager, this field does not display.
Use SNTP to update time	Daily SNTP updates of the system time

Field	Description
Power State	Current power state of the AirLink device: • Initial — The device is in the initial 5 minutes since power up, so power down event will be ignored • ON — Regular power on, a power down is not pending • Low Cancellable — Power down is pending but still cancellable if the power down trigger goes away • Low Pending 1 and Low Pending 3 — Power down is pending, any device tasks are gracefully preparing for the power down • Low Final — Power down is imminent • Low — Power is down
Engine Hours	Time the engine has been running. Depending on your configuration, this is based on: • Voltage on the Power Pin from the vehicle battery (Engine Hours On Voltage Level) • Voltage on the Ignition Sense Pin (Engine Hours Ignition Enable)

GPS

The GPS (Global Positioning System) tab provides AirLink device location and movement information for use with tracking applications.

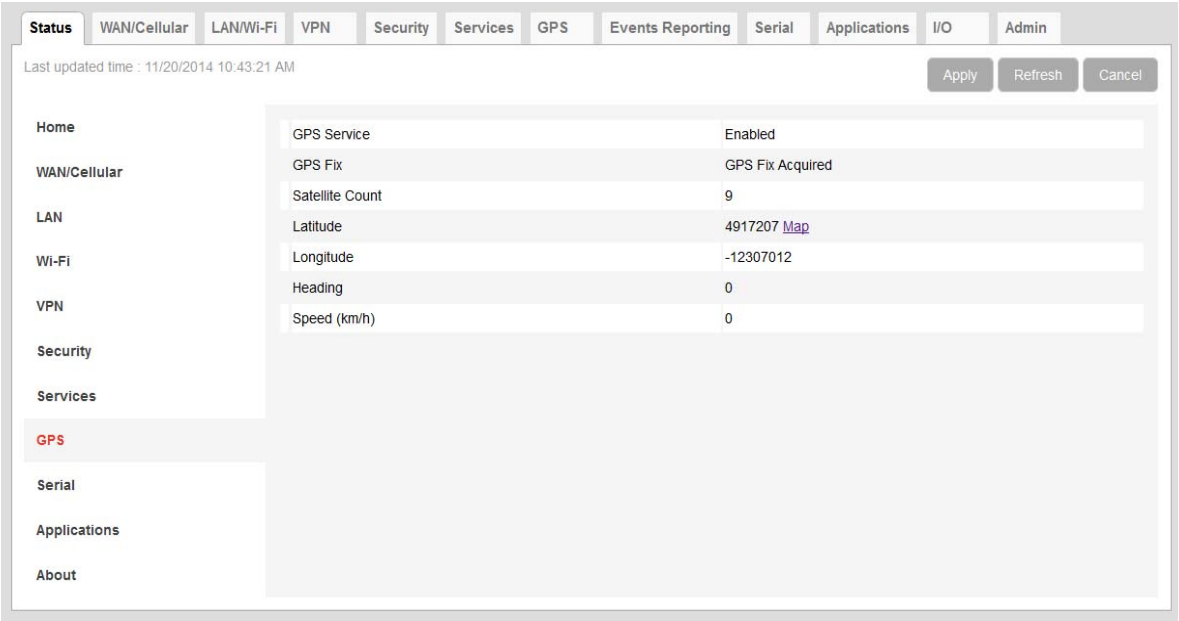


Figure 3-14: ACEmanager: Status > GPS

Field	Description
GPS Service	Status of the GPS Service • Enabled • Disabled
The remainder of the fields only appear if GPS Service is enabled.	

Field	Description
GPS Fix	Status of the GPS fix • No GPS Fix • GPS Fix Acquired • GPS WAAS Fix— Wide Area Augmentation System GPS fix
Satellite Count	Number of satellites the GPS receiver detects
Latitude	Latitude of the GPS receiver Click the Map link to view the current location of the device, using Google Maps™.
Longitude	Longitude of the GPS receiver
Heading	Direction in which the AirLink device is moving. No configuration is needed for Heading or Speed; these are calculated automatically.
Speed (km/h)	Speed (in kilometers per hour)

Serial

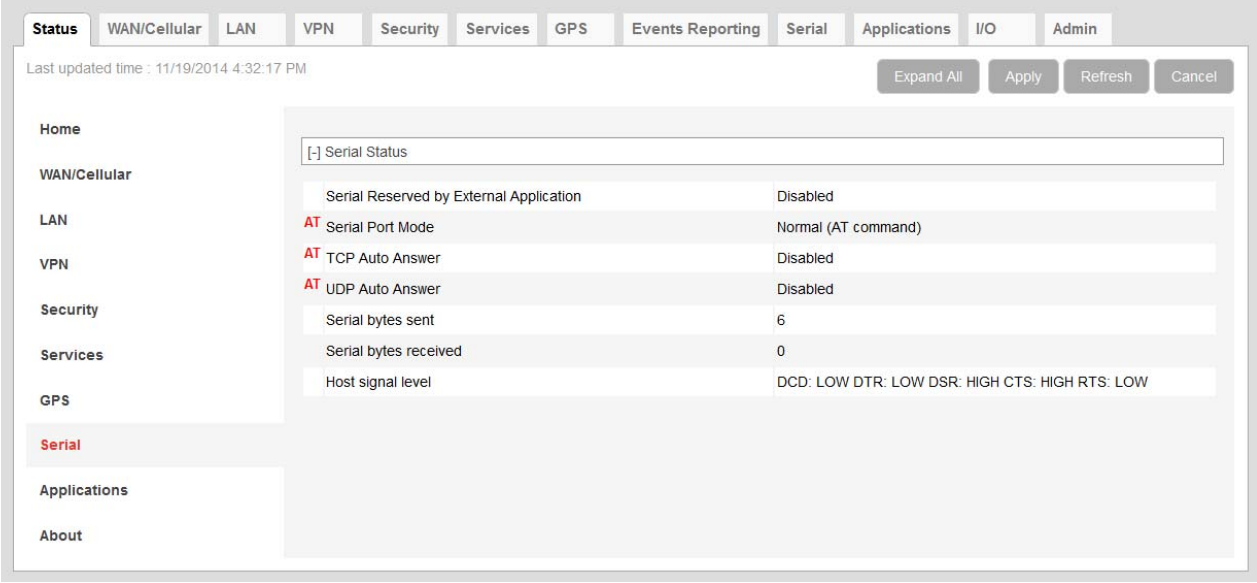
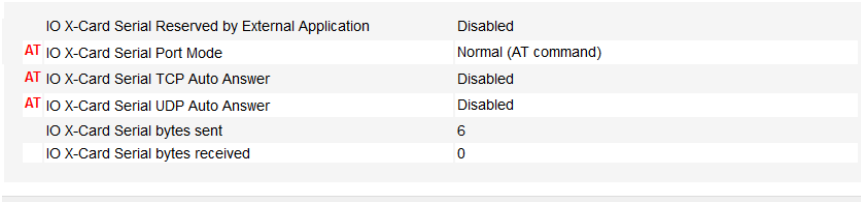


Figure 3-15: ACEmanager: Status > Serial

Field	Description
Serial Reserved by External	Reservation status of the serial port: • Enabled—The serial port is reserved for ALEOS Application Framework (ALEOS AF), and cannot be used for any other serial-related ALEOS features. • Disabled— The serial port is available for non-ALEOS AF, serial-related ALEOS features. To reserve the serial port for ALEOS AF, go to Applications > ALEOS Application Framework > Serial Port Reserved. (See ALEOS Application Framework on page 314.)
Serial Port Mode	Default power-up mode for the serial port. When the AirLink device is power-cycled, the serial port enters the mode specified by this command after 5 seconds.
Autologin reverse telnet	This field only appears when reverse telnet is selected as the Serial Port Mode. Status of autologin for reverse telnet. For more information, see Reverse Telnet/SSH on page 279.
TCP Auto Answer	This parameter determines how the AirLink device responds to an incoming TCP connection request. The AirLink device remains in AT Command mode until a connection request is received. DTR must be asserted (S211=1 or &D0) and the device must be set for a successful TCP connection. The AirLink device sends a “RING” string to the host. A “CONNECT” sent to the host indicates acknowledgment of the connection request and the TCP session is established. • Disabled (default) • Enabled
UDP Auto Answer	How UDP auto answer (half-open) mode is configured • Normal mode • Enable UDP auto answer mode
Serial bytes sent	Number of bytes sent over serial port to host
Serial bytes received	Number of bytes received over serial port from host
Serial Signal Level	Status of the following parameters related to the host signal level: • DCD—Data Carrier Detect—Control signal to the PC • DTR—Data Terminal Ready—Used to establish a connection • DSR—Data Set Ready—Used to establish a connection • CTS—Clear to Send—Data flow control • RTS—Request to Send—Data flow control Each parameter can have a value of LOW (signal not asserted) or HIGH (signal being asserted). The first three parameters (DCD, DTR, and DSR) may be helpful for troubleshooting. If the values shown for these parameters are not as expected: 1. Press Refresh to ensure you have the latest values. 2. Check the cable connections. *Note: ACEmanager does not update dynamically. Press Refresh to view the current values.*

Field	Description
I/O X-Card Serial These fields apply only to GX Series devices with an I/O X-Card installed. 	
I/O X-Card Serial Reserved by External	Reservation status of the I/O X-Card serial port: • ON—The serial port is reserved for ALEOS Application Framework (ALEOS AF), and cannot be used for any other serial-related ALEOS features. • OFF— The serial port is available for non-ALEOS AF, serial-related ALEOS features. To reserve the serial port for ALEOS AF, go to Applications > ALEOS Application Framework > Serial Port Reserved. (See ALEOS Application Framework on page 314.)
I/O X-Card Serial Port Mode	Default power-up mode for the I/O X-Card serial port. When the AirLink device is power-cycled, the serial port enters the mode specified by this command after 5 seconds.
I/O X-Card Serial TCP Auto Answer	This parameter determines how the AirLink device responds to an incoming TCP connection request on the I/O X-Card serial port. The AirLink device remains in AT Command mode until a connection request is received. DTR must be asserted (S211=1 or &D0) and the device must be set for a successful TCP connection. The AirLink device sends a “RING” string to the host. A “CONNECT” sent to the host indicates acknowledgment of the connection request and the TCP session is established. • Disabled (default) • Enabled
I/O X-Card Serial UDP Auto Answer	How UDP auto answer (half-open) mode on the I/O X-Card serial port is configured: • Normal mode • Enable UDP auto answer mode
I/O X-Card Serial bytes sent	Number of bytes sent over the I/O X-Card serial port to host
I/O X-Card Serial bytes received	Number of bytes received over the I/O X-Card serial port from host

Applications

The Applications section of the Status group provides information on the status of the Garmin device and data service.

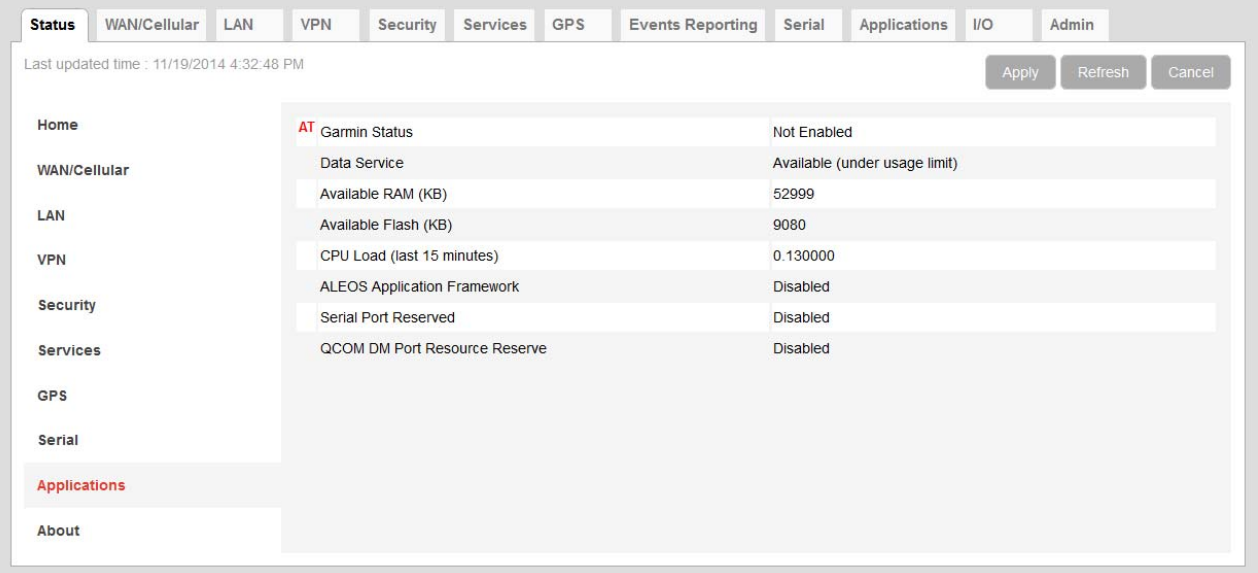


Figure 3-16: ACEmanager: Status > Applications

Field	Description
Garmin Status	State of the connection to the Garmin device when it is enabled. This field is blank when the Garmin device is disabled.
Data Service	Data Service field displays “Available (under usage limit)” if the configured usage limit has not been exceeded.
Available RAM (KB)	Available RAM in kilobytes (1000 bytes), updated every 30 seconds
Available Flash (KB)	Available Flash on the user partition in kilobytes (1024 bytes), updated every 30 seconds
CPU Load (Last 15 minutes)	CPU load, averaged over the last 15 minutes and updated every 30 seconds The CPU load relates to how many applications are attempting to execute in parallel over the 15-minute period. If the load is greater than 1, some applications are waiting for CPU capacity to become available and may be delayed in launching.
ALEOS Application Framework	Whether ALEOS Application Framework is enabled or disabled
Serial Port Reserved	Reservation of the serial port: • Disable (default) • Enable
QCOM DM Port Resource Reserve	Reservation of the QCOM DM port: • Disable (default) • Enable

About

The About section of the Status group provides basic information about the AirLink device. The fields for this section provide the same information for the CDMA, GSM, and LTE wireless standards.

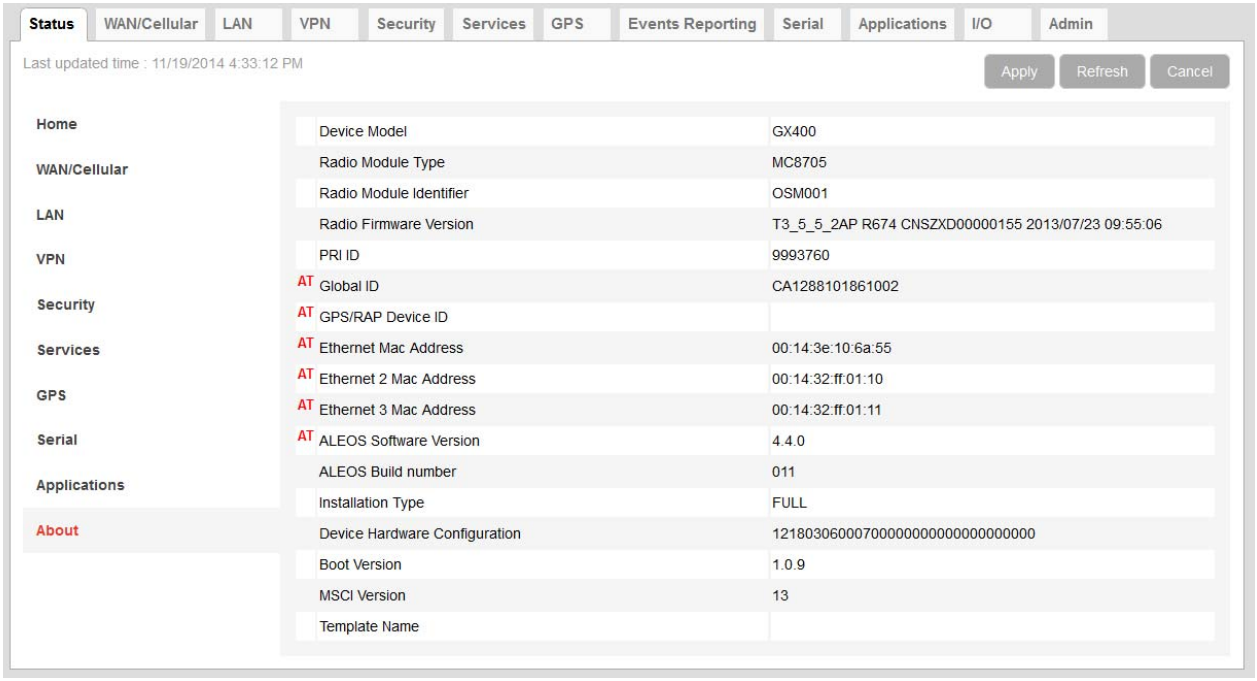


Figure 3-17: ACEmanager: Status > About

Field	Description
Device Model	Model of the device (e.g., LS300, GX400,)
Radio Module Type	Model number of the internal cellular radio module (e.g. MC7700, SL5011)
Radio Module Identifier	Identifier for the internal mobile radio module
Radio Firmware Version	Firmware version in the radio module
PRI ID	Product Release Instructions ID number
Global ID	Device ID used by ALEOS to identify itself for various management applications
GPS/RAP Device ID	Device ID used by GPS/RAP and other reporting
Ethernet Mac Address	MAC address of the main Ethernet port
Ethernet 2 Mac Address	MAC address of Ethernet port 2 on the Dual Ethernet X-Card (Only appears if the device has a Dual Ethernet X-Card installed)
Ethernet 3 Mac Address	MAC address of Ethernet port 3 on the Dual Ethernet X-Card (Only appears if the device has a Dual Ethernet X-Card installed)

Field	Description
ALEOS Software Version	Version of ALEOS software running on the AirLink device
ALEOS Build number	Build number for the ALEOS Software
Device Hardware Configuration	AirLink device's hardware configuration
Boot Version	Version of boot code installed in the device
MSCI Version	MSCI version of the ALEOS internal configuration database
Template Name	If you have installed a custom-named template, the name appears here. Otherwise, the field is blank.
Module CDMA check	This field only appears on AirLink devices with radio module MC7750. Shows the status of the module CDMA parameters. Possible values are: • Success—Module CDMA parameters are valid. • Fail—Module CDMA parameters are not valid. *Note: If the check fails, this field is empty. (Status is unknown.)*

4: WAN/Cellular Configuration

4

The WAN/Cellular section allows changes to the cellular connection and main operating mode of the AirLink device. The options available in ACEmanager depend on the type of technology your AirLink device use. Refer to the appropriate section for your device:

- CDMA
- GSM on page 78
- LTE—Fallback to EV-DO on page 83
- LTE—Fallback to HSPA on page 87

CDMA

This section applies to GX400 devices with radio module MC5728 and LS300 devices with radio module SL5011.

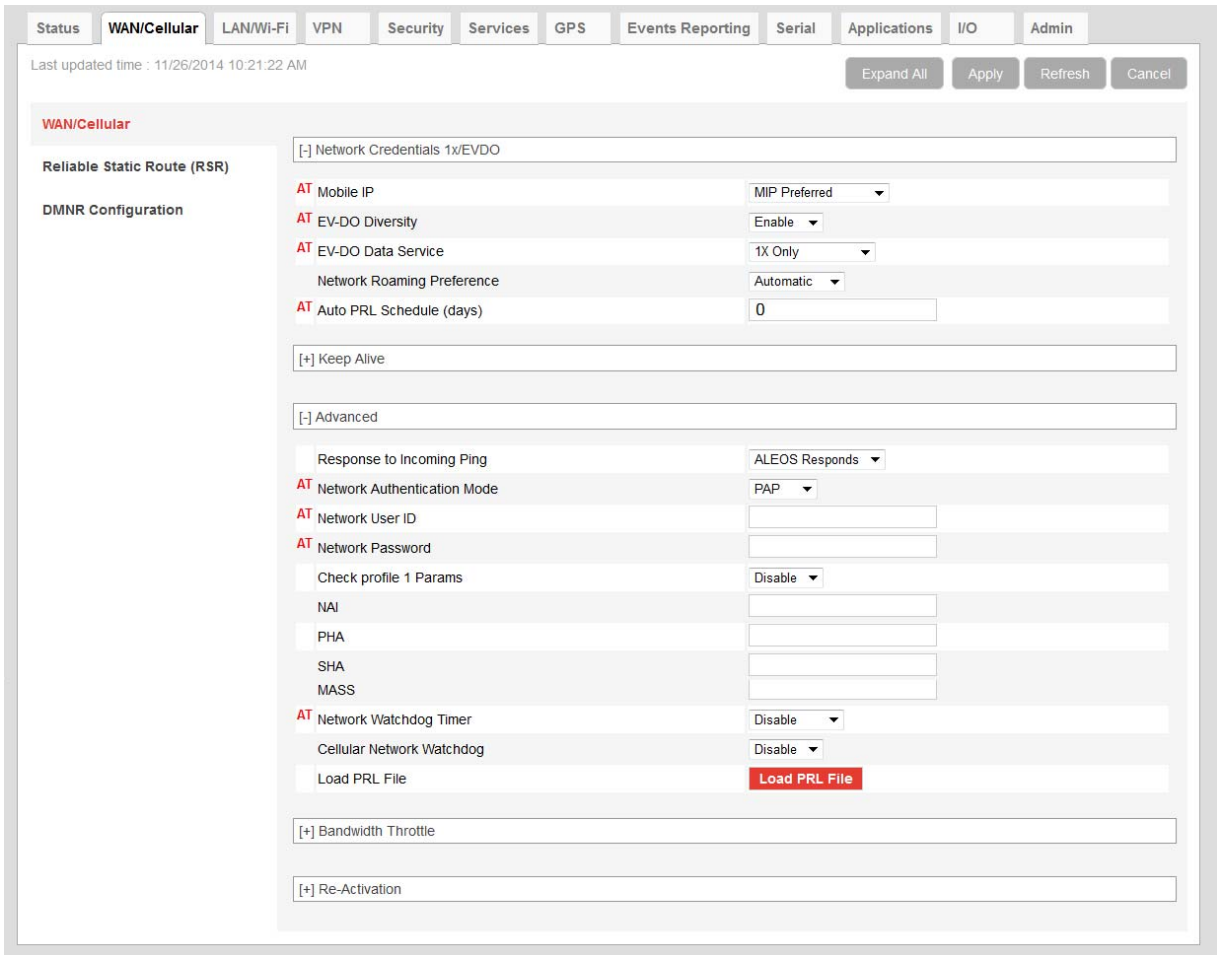


Figure 4-1: ACEmanager: WAN/Cellular —1x/EV-DO

Field	Description
Network Credentials 1x/EVDO	
Mobile IP	Mobile IP (MIP) Preferences. On a Mobile IP network, a device connects to the network using PPP. During the negotiation process the AirLink device is NOT required to present a username and password to authenticate because the authentication parameters are stored in the device itself. • Disabled, SIP only • MIP Preferred • MIP Only Default: MIP is used when available with a fall back to SIP. *Note: Your account with your Mobile Network Operator may not support all three of these options. check with your Mobile Network Operator as to which one should be used.*
EV-DO Diversity	EV-DO Diversity allows two antennas to provide a more consistent connection. • Disable • Enable (default) If you are not using a diversity antenna, diversity should be disabled. *Note: This field is not available in all AirLink devices.*
EV-DO Data Service	Change the allowable network type: • EV-DO Preferred — can “fall back” on CDMA/1x • EV-DO Only — fall back disabled • 1x Only — EV-DO disabled *Note: For most users, it’s best to leave the default setting (EV-DO Preferred). When this option is selected, your AirLink device connects to an EV-DO network if it is available and falls back to a CDMA 1x network if EV-DO service is not available. If you choose another option and the selected network is not available, the device will not be able to connect to the cellular network. For example, if you select EV-DO Only and you are in an area where there is no EV-DO network available, the device will not be able to connect to a cellular network until you change this setting.*
Network Roaming Preference	Allows you to control whether or not roaming (connecting to a mobile broadband network other than that of your Mobile Network Operator). Options are: • Automatic—The device connects to the home network if it is available and to another Mobile Network Operator’s network if the home network is not available (for example you are outside the coverage area). Note: Roaming charges may apply. • Home Only—The device only connects to the home network. If the home network is not available (for example, if you are outside the coverage area) the device does not connect until the home network is available again.
Auto PRL Schedule (days)	Indicates the PRL update schedule • 0=disable
Keep Alive (See Keepalive on page 92.)	

Field	Description
Advanced	
Response to Incoming Ping	When a ping is received by the device from a remote location, the Response to Incoming Ping redirects it to the selected location. • No response: the incoming ping is completely ignored • ALEOS Responds (default): ALEOS returns to the Ping response. • Pass to Host: The ping is forwarded to the DMZ host with any response from the host forwarded back to the OTA location. If no host is connected, there is no ping response. *Note: Some Mobile Network Operators may block all ICMP traffic on their network. A ping sent to the device from a remote location is not received.*
Network Authentication Mode	Specifies the authentication method to use in the network PPP session. Options are: • None • CHAP • PAP (default)
Network User ID	Network User ID The login that is used to login to the cellular network, when required. • Maximum 128 characters
Network Password	Network Password is the password that, when required, is used to login to the cellular network. • Maximum 30 characters
Check profile 1 Params	Enables checking and updating the Profile 1 Parameters. Options are: • Enable • Disable (default) *Not all Mobile Network Operators or account types support this feature.*
NAI	Sets the Network Access ID Not all Mobile Network Operators or account types support this feature.
PHA	Sets the IP address of the primary home agent Not all Mobile Network Operators or account types support this feature.
SHA	Sets the IP address of the secondary home agent Not all Mobile Network Operators or account types support this feature.
MHSS	Sets the home agent shared secret key Not all Mobile Network Operators or account types support this feature.
MASS	Sets the AAA shared secret key Not all Mobile Network Operators or account types support this feature.
Network Watchdog (minutes)	Network connection watchdog If there is no WWAN/Cellular network connection for the number of minutes configured in this field, the device reboots. This feature cannot be disabled. • 5–255 minutes (allowed values) • 120 minutes (default)
Load PRL File	The Load PRL File button allows you to download a Preferred Roaming List.
Update PRL	The Update PRL button allows you to update your Preferred Roaming List.

Field	Description
Update Profile	The Update Profile button allows you to update the profile of your Preferred Roaming List.
Re-Activation	
Re-Activate Cellular Account	See Re-Activation on page 96.
Re-Activation Status (See Re-Activation on page 96.)	
Bandwidth Throttle (See Bandwidth Throttle on page 97.)	

GSM

This section applies to GX400 devices with radio module MC8705 and LS300 devices with radio module SL8090 or SL8092.

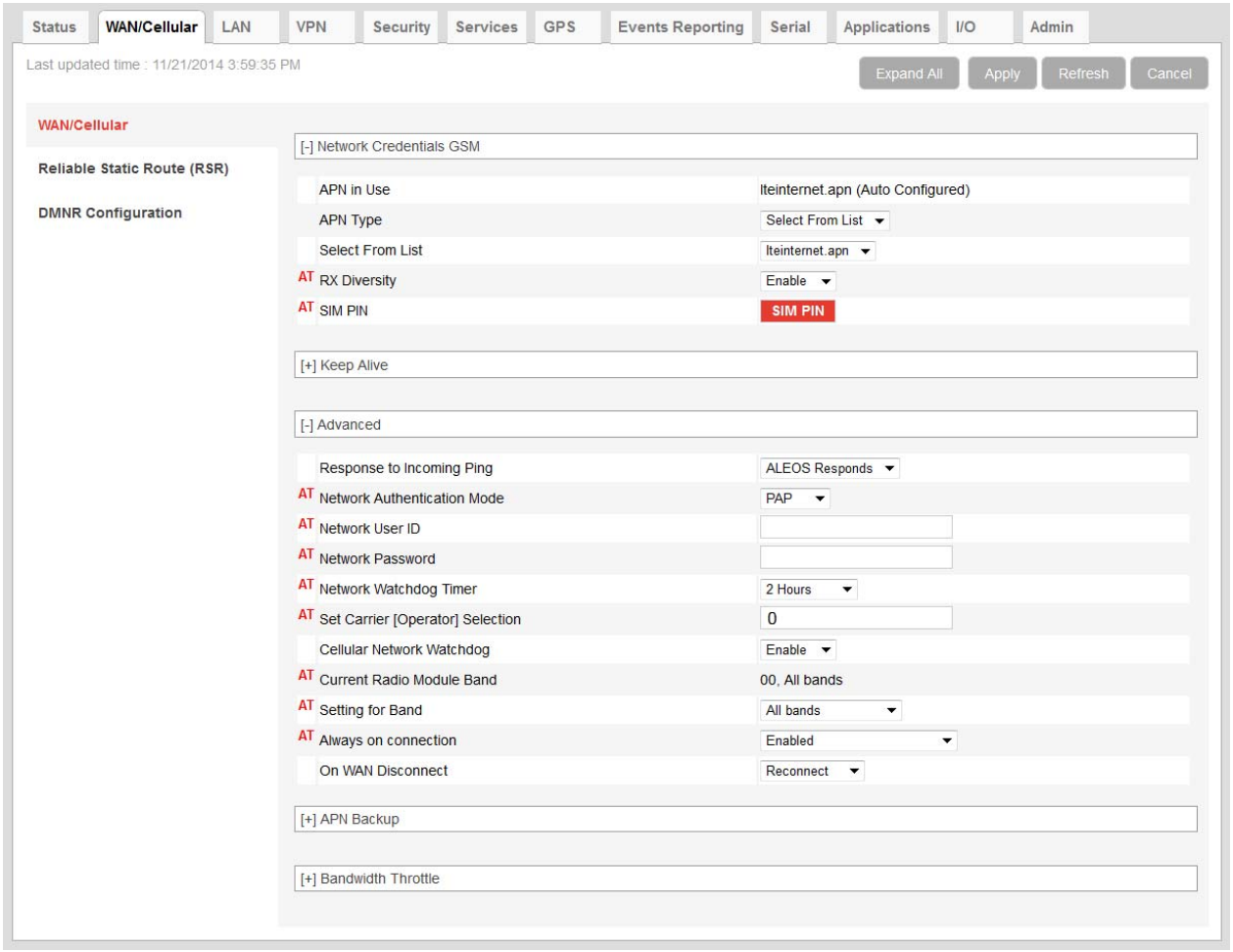
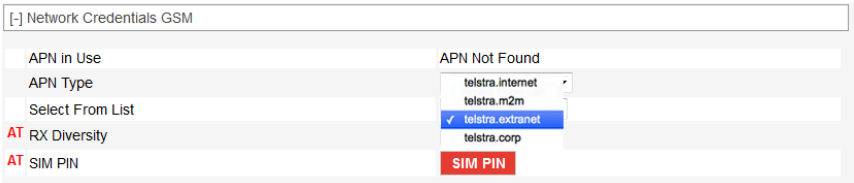


Figure 4-2: ACEmanager: WAN/Cellular—GSM

Field	Description
Network Credentials GSM	
Note: The first time you power on the AirLink device, ALEOS automatically selects the most commonly used APN for the Mobile Network Operator identified on the inserted SIM card. This APN appears as the first item in the Select from List field. It is used if no other APN is selected or configured.	
APN in Use	The APN in use for the current mobile network connection. When you power on the AirLink device, the APN the device is using for authentication on the mobile network is displayed. • If a User Entered APN is configured, the User Entered APN is displayed. • If there is no User Entered APN configured, an automatically-selected APN is displayed. • When the Backup APN is configured, the APN in Use displays the configured Backup APN when it is being used for authentication on the mobile network. If ALEOS is unable to find the appropriate APN to use, contact your Mobile Network Operator for the APN and enter it in the User Entered APN field.
APN Type	If you do not want to use the automatically-selected APN, use this field to choose how you want to enter that APN. Options are: • Select From List — When selected, the Select from List field appears, which allows you to select the desired APN from the list. • User Entry — When selected, the User Entered APN field appears, which allows you to type in the desired APN.
User Entered APN	Appears when the APN Type is “User Entry”. If your Mobile Network Operator has advised you to use an APN other than the automatically-selected APN, enter that APN in this field (maximum 128 characters). An APN entered in this field takes priority over the automatically-selected APN. *Note: If you reset the device to factory defaults, you have the option to preserve the custom APN, if entered. See Reset Mode on page 328.*
Select From List	Appears when the APN Type is “Select from List”. Click in this field to display a drop-down list of available APNs. Select the desired APN from the list. 
RX Diversity	Allows two antennas to provide a more consistent connection • Disable • Enable (default) If you are not using a diversity antenna, diversity should be disabled. *Note: This field is not available in all AirLink devices.*

Field	Description
SIM PIN	Click this button to configure the PIN stored on the AirLink device. For more information, see SIM PIN on page 93.
Keep Alive (See Keepalive on page 92.)	
Advanced	
Response to Incoming Ping	When a ping is received by the device from a remote location, the Response to Incoming Ping redirects it to the selected location. • No response: the incoming ping is completely ignored • ALEOS Responds (default): ALEOS responds to the Ping response. • Pass to Host: The ping is forwarded to the DMZ host with any response from the host forwarded back to the OTA location. If no host is connected, there is no ping response. *Note: Some Mobile Network Operators may block all ICMP traffic on their network. A ping sent to the device from a remote location is not received.*
Network Authentication Mode	Specifies the authentication method to use in the network PPP session. Options are: • None • CHAP • PAP (default)
Network User ID	Network User ID The login that is used to login to the cellular network, when required. • Maximum 128 characters
Network Password	Network Password is the password that, when required, is used to login to the cellular network. • Maximum 30 characters
Network Watchdog Timer	Network Watchdog Timer If there is no WAN connection for the time configured in this field, the device reboots. Options are: • Disable—When this field and the Cellular Network Watchdog field are set to Disable, the device never reboots as a result of lack of network connectivity. • 5 Minutes • 10 Minutes • 15 Minutes • 30 Minutes • 45 Minutes • 1 Hour • 2 Hours (default) • 3 Hours • 4 Hours

Field	Description
Set Carrier (Operator) Selection	Manually specify an operator. Enter the desired parameters in the following format: mode[,format[,oper]] • mode= 0: Automatic — any affiliated carrier [default] • mode= 1: Manual — use only the operator <oper> specified • mode= 4: Manual/Automatic — if manual selection fails, goes to automatic mode • format= 0: Alphanumeric (“name”) • format= 2: Numeric • oper=”name” See also +COPS and *NETOP? *Note: Not all carriers or accounts allow specifying the operator. If the carrier doesn't support it, this command may appear to fail.*
Cellular Network Watchdog	Cellular Network Watchdog Options are: • Enable—When this Watchdog is enabled, the device reboots after several attempts to authenticate on the network fail. (default) • Disable—When this field and the Network Watchdog Timer field are both set to Disable, the device never reboots as a result of lack of network connectivity.
Current Radio Module Band	Band reported by the radio module.
Setting for Band	This feature enables advanced users to select the RF band range or technology the AirLink device uses. Most of the time it’s best to leave this field at the default setting (All bands) but there may be times when you want to select a band range or technology that you know is more stable in the region where the AirLink device is located. The list of options displayed depends on the radio module in your device and its configuration. Possible options include: • All bands (default) • GSM 900/1800 • GSM ALL • WCDMA ALL • WCDMA 900/2100 *Note: For some Mobile Network Operator SIM Cards, you may need to set the radio band before installing the SIM card.*

Field	Description

Always on connection	This field is intended for OpenSIM devices on the Vodafone network.
	This option allows you to configure the AirLink device to use minimal wireless network resources when there has not been any outgoing WAN network traffic.
	• Enabled—The AirLink device maintains a mobile network data connection. (default)
	• Disabled—Connect on traffic—The AirLink device only establishes a mobile network data connection:
	  • When there is network traffic
	  • If SMS Wakeup is configured and the device receives the specified type of SMS (For information on configuring SMS Wakeup, see SMS Wakeup on page 210.)
	*Note: You can also use AT*RADIO_CONNECT to switch the cellular network connection on and off. See *RADIO_CONNECT on page 400.*

Connection timeout (minutes)	This field is intended for OpenSIM devices on the Vodafone network. This field only appears when Always on Connection is set to Disable - Connect on traffic, and defines the timeout period for Always on connection. If there is no outgoing packet through the WAN interface during the period set in this field (in minutes), the AirLink device disables the WAN connection. This timer is triggered after every outgoing packet, except AT*IPPINGFORCE keep alive packets. • 2–65535 minutes (Default is 2.) *Note: You can also use AT*TRAFWUPTOUT to set the timeout period. See *TRAFWUPTOUT on page 401.*
On WAN Disconnect	If a disconnect from the Mobile Network Operator occurs: • Reconnect (default) • Reset Radio — ALEOS resets the radio after a Mobile Network Operator disconnect.
APN Backup (See Backup APN on page 96.)	
Bandwidth Throttle (See Bandwidth Throttle on page 97.)	

LTE—Fallback to EV-DO

This section applies to GX440devices with radio module MC7750.

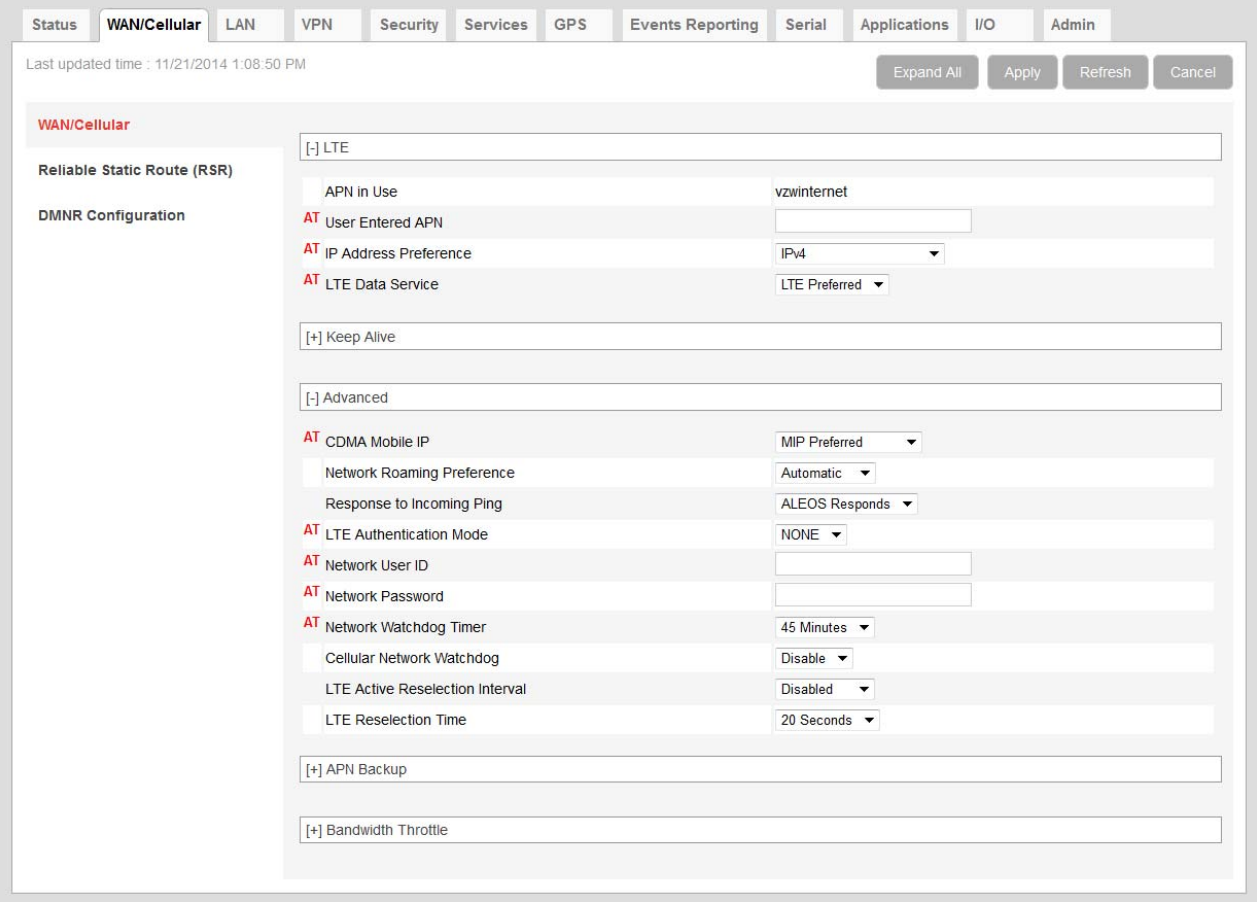
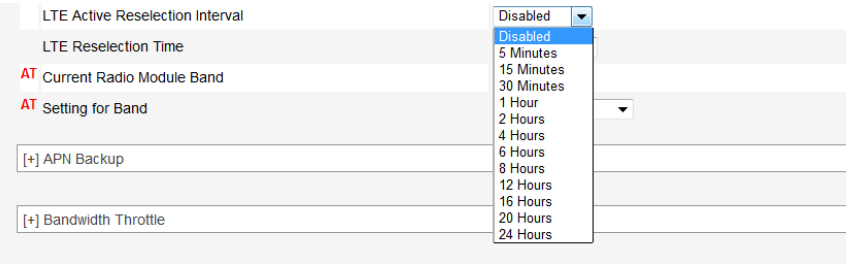


Figure 4-3: ACEmanager: WAN/Cellular > LTE

Field	Description
LTE (falls back to EV-DO)	
Note: The first time you power on the AirLink device, ALEOS automatically selects the most commonly used APN for the Mobile Network Operator identified on the inserted SIM card. This APN is used if no other APN is selected or configured.	

Field	Description
APN in Use	The APN in use for the current mobile network connection. When you power on the AirLink device, the APN the device is using for authentication on the mobile network is displayed. • If a User Entered APN is configured, the User Entered APN is displayed. • If there is no User Entered APN configured, an automatically-selected APN is displayed. • When the Backup APN is configured, the APN in Use displays the configured Backup APN when it is being used for authentication on the mobile network. If ALEOS is unable to find the appropriate APN to use, contact your Mobile Network Operator for the APN and enter it in the User Entered APN field.
User Entered APN	If your Mobile Network Operator has advised you to use an APN other the automatically-selected APN, enter that APN in this field (maximum 128 characters). The APN entered in this field takes priority over the automatically-selected APN. *Note: If you are activating a GX440 device on the LTE network using a SIM card for an account with special properties, such as a static IP APN:* **1.** *Enter the static IP APN in this field.* **2.** *Click Apply.* **3.** *Click Reboot.* *Note: If you reset the device to factory defaults, you have the option to preserve the custom APN, if entered. See Reset Mode on page 328.*
IP Address Preference	This feature is only supported on the AirLink GX440. Use this field to select the preferred IP Address version. To use IPv6, it must be supported by your Mobile Network Operators and your account (SIM and APN). *Note: If you are configuring this feature on a Verizon Wireless network, IPv6 is supported on the vzwinternet standard APN, but is not supported on static IP APNs, such as we01.vzwstatic.* Options are: • IPv4—When the device connects to the cellular network, it is assigned only an IPv4 address. • IPv4 and IPv6 Gateway—When the device connects to the cellular network, it is assigned an IPv4 address and an IPv6 address. The IPv6 address and routing information are passed to the LAN clients so that they can acquire IPv6 addresses and pass IPv6 traffic over the cellular network. *Note: The LAN client must have IPv6 enabled and must be configured to use SLAAC (Stateless address auto configuration).* The IPv6 address and routing information, and DNS servers are passed to the LAN clients via SLAAC. *Note: Other than routing IPv6 packets between the WAN and the LAN, no other AirLink features are supported on IPv6.* The IP addresses are displayed on the Status > Home and Status > WAN screens.

Field	Description
LTE Data Service	For LTE, fallback to EV-DO networks. Options are: • LTE Preferred (default)—EV-DO is used when LTE service is not available • CDMA Only • LTE Only *Note: For most users, it's best to leave the default setting (LTE Preferred). When this option is selected, your AirLink device connects to an LTE network if it is available and falls back to an EV-DO network if LTE service is not available. If you choose another option and the selected network is not available, the device will not be able to connect to the cellular network. For example, if you select LTE Only and you are in an area where there is no LTE network available, the device will not be able to connect to a cellular network until you change this setting.*
Keep Alive (See Keepalive on page 92.)	
Advanced	
CDMA Mobile IP	Options are: • MIP Preferred (default) • Disabled, SIP Only • MIP Only
Network Roaming Preference	Automatic option allows home or home preferred network preference. Options are: • Automatic (default) • Home Only
Response to Incoming Ping	When a ping is received by the device from a remote location, the Response to Incoming Ping redirects it to the selected location. • No response: the incoming ping is completely ignored • ALEOS Responds (default): ALEOS responds to the ping. • Pass to Host: The ping is forwarded to the DMZ host with any response from the host forwarded back to the OTA location. If no host is connected, there is no ping response. *Note: Some Mobile Network Operators may block all ICMP traffic on their network. A ping sent to the device from a remote location is not received.*
LTE Authentication Mode	Specifies the authentication method to be used in the network PPP session. Options are: • NONE (default) • PAP • CHAP
Network User ID	Network User ID The ID that is used to login to the cellular network, when required. • Maximum 128 characters
Network Password	Network Password is the password that, when required, is used to login to the cellular network. • Maximum 30 characters

Field	Description
Network Watchdog (minutes)	Network connection watchdog If there is no network connection for the number of minutes configured in this field, the device reboots. This feature cannot be disabled. • 5–255 minutes (allowed values) • 120 minutes (default)
LTE Active Reselection Interval	Use this field to set the LTE Active Reselection Interval timer. When an LTE AirLink device is connected to a non-LTE network, it may not handover to an LTE network (even if one becomes available) if data is being continuously transmitted or received. When the LTE Active Reselection Interval timer is configured, the AirLink device performs a radio reset if it is connected to a non-LTE network for the configured time. After the reset, the radio module performs a full network scan and may revert to an LTE network, if one is available. *Note:* • *The reset causes any active data session to terminate and the radio to lose its IP address.* • *If the AirLink device reverts back an LTE network before the timer expires, no radio reset occurs.* • *This feature should be disabled when the device is located in an area where it is unlikely to find an LTE network.* To use this feature: 1. Ensure that the LTE Data Service field is set to LTE Preferred. 2. From the drop-down menu in the LTE Active Reselection Interval field, select how long the AirLink device is not on an LTE network before the reselection process begins. (Disabled is the default.)  3. Click Apply. 4. Reboot the device.
APN Backup (See Backup APN on page 96.)	
Bandwidth Throttle (See Bandwidth Throttle on page 97.)	

LTE—Fallback to HSPA

This section applies to GX440 devices with radio modules MC7700.

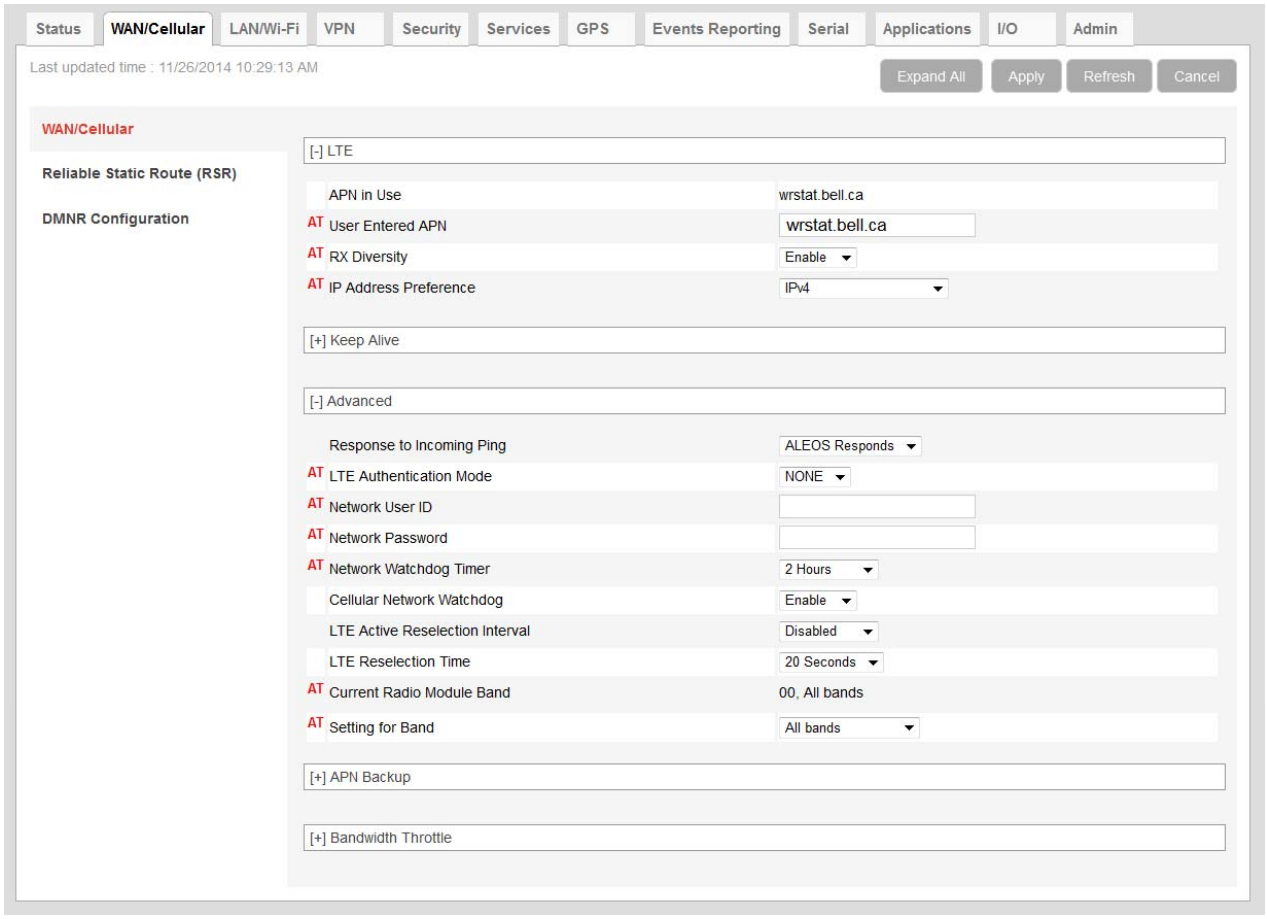


Figure 4-4: ACEmanager: WAN/Cellular—LTE - Fallback to HSPA

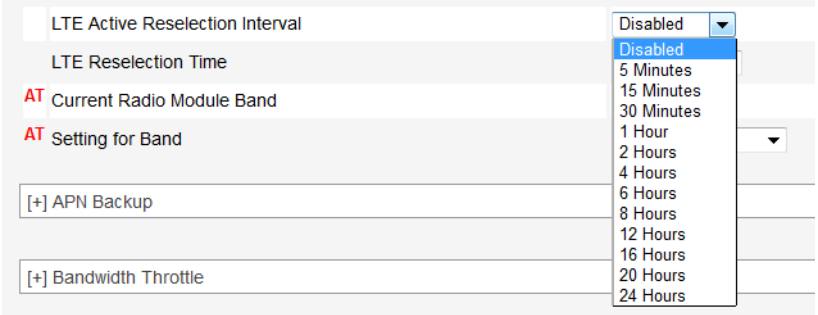
Field	Description
LTE (Falls back to HSPA)	
Note: The first time you power on the AirLink device, ALEOS automatically selects the most commonly used APN for the Mobile Network Operator identified on the inserted SIM card. This APN is used if no other APN is selected or configured.	

Field	Description
APN in Use	The APN in use for the current mobile network connection. When you power on the AirLink device, the APN the device is using for authentication on the mobile network is displayed. • If a User Entered APN is configured, the User Entered APN is displayed. • If there is no User Entered APN configured, an automatically-selected APN is displayed. • When the Backup APN is configured, the APN in Use displays the configured Backup APN when it is being used for authentication on the mobile network. If ALEOS is unable to find the appropriate APN to use, contact your Mobile Network Operator for the APN and enter it in the User Entered APN field.
User Entered APN	If your Mobile Network Operator has advised you to use an APN other than the automatically-selected APN, enter that APN in this field (maximum 128 characters). The APN entered in this field takes priority over the automatically-selected APN. *Note: If you are activating a GX440 device on an LTE network using a SIM card for an account with special properties, such as a static IP APN:* **1.** *Enter the static IP APN in this field.* **2.** *Click Apply.* **3.** *Click Reboot.* *Note: If you reset the device to factory defaults, you have the option to preserve the custom APN, if entered. See Reset Mode on page 328.*
IP Address Preference	This feature is only supported on the AirLink GX440. Use this field to select the preferred IP Address version. To use IPv6, it must be supported by your Mobile Network Operators and your account (SIM and APN). Options are: • IPv4—When the device connects to the cellular network, it is assigned only an IPv4 address. • IPv4 and IPv6 Gateway—When the device connects to the cellular network, it is assigned an IPv4 address and an IPv6 address. The IPv6 address and routing information are passed to the LAN clients so that they can acquire IPv6 addresses and pass IPv6 traffic over the cellular network. *Note: The LAN client must have IPv6 enabled and must be configured to use SLAAC (Stateless address auto configuration).* The IPv6 address and routing information, and DNS servers are passed to the LAN clients via SLAAC. *Note: Other than routing IPv6 packets between the WAN and the LAN, no other AirLink features are supported on IPv6.* The IP addresses are displayed on the Status > Home and Status > WAN screens.

Field	Description
RX Diversity	Allows two antennas to provide a more consistent connection • Disable • Enable (default) If you are not using a diversity antenna, diversity should be disabled. *Note: This field is not available in all AirLink devices.*
Keep Alive (See Keepalive on page 92.)	
Advanced	
Response to Incoming Ping	When a ping is received by the device from a remote location, the Response to Incoming Ping redirects it to the selected location. • No response: the incoming ping is completely ignored • ALEOS Responds (default): ALEOS responds to the ping. • Pass to Host: The ping is forwarded to the DMZ host with any response from the host forwarded back to the OTA location. If no host is connected, there is no ping response. *Note: Some Mobile Network Operators may block all ICMP traffic on their network. A ping sent to the device from a remote location is not received.*
LTE Authentication Mode	Specifies the authentication method to be used in the network PPP session. Options are: • NONE (default) • PAP • CHAP
Network User ID	Network User ID The ID that is used to login to the cellular network, when required. • Maximum 128 characters
Network Password	Network Password is the password that, when required, is used to login to the cellular network. • Maximum 30 characters
Network Watchdog (minutes)	Network connection watchdog If there is no network connection for the number of minutes configured in this field, the device reboots. This feature cannot be disabled. • 5–255 minutes (allowed values) • 120 minutes (default)

Field	Description

LTE Active Reselection Interval	This feature assists the device to revert back to an LTE network if one becomes available.
	When an LTE AirLink device is connected to a non-LTE network, it may not handover to an LTE network (even if one becomes available) if data is being continuously transmitted or received.
	When the LTE Active Reselection Interval timer is configured, the AirLink device temporarily halts uplink data if it is connected to a non-LTE network for the configured time. This allows the radio module to go idle and reconnect to an LTE network, if one is available.
	Note:
	• *The current active data session continues, but data is dropped for a period equal to (or less than) the value set in the LTE Reselection Time field.*
	• *If the AirLink device reverts back an LTE network before the timer expires, reselection does not occur.*
	• *If the AirLink device does not revert back an LTE network before the timer expires, the reselection process begins and runs for the length of time configured in the LTE Reselection Time field.*
	• *If the LTE signal that the AirLink device receives is weaker than the HSPA+ signal, the device may not revert to LTE, depending on the local network characteristics.*
	• *This feature should be disabled:*
	  • *If the SIM in the device is not provisioned to work on an LTE network*
	  • *If the option in the Setting for Band field forces the band to be something other than LTE*
	  • *If the device is roaming*

LTE Active Reselection Interval (Continued)	To use this feature: 1. Ensure that the Setting for Band field is set to an option that includes LTE (All bands, Europe, North America, or LTE ALL). 2. From the drop-down menu in the LTE Active Reselection Interval field, select how long the AirLink device is not connected to an LTE network before the reselection process begins. (Disabled is the default.)  3. If desired, change the default value in the LTE Reselection Time field. 4. Click Apply. 5. Reboot the device.

Field	Description
LTE Reselection Time	Use this field to set how long the device radio should attempt to find and connect to an LTE network (i.e. how long the reselection process described in LTE Active Reselection Interval should last). Data transmitted during the reselection process is dropped. Common Transport Layer protocols such as TCP/IP will retransmit any lost packets. *Note: The length of time that packets are dropped could be shorter than the time set in this field if the device finds and connects to an LTE network before the time expires, or if the reselection process fails before the time expires because it is interrupted by incoming traffic.* Options are: • 15 seconds • 20 seconds (default) • 25 seconds • 30 seconds
Current Radio Module Band	Band reported by the radio module.
Setting for Band	This feature enables advanced users to select the RF band range or technology the AirLink device uses. Most of the time it's best to leave this field at the default setting (All bands) but there may be times when you want to select a band range or technology that you know is more stable in the region where the AirLink device is located. The list of options displayed depends on the radio module in your device and its configuration. Possible options include: • All bands (default) • Europe 3G* • North America 3G* • Europe 2G* • GSM ALL* • Europe • North America • WCDMA ALL* • LTE ALL * If you select this setting, disable LTE Active Reselection Interval (see page 90).
APN Backup (See Backup APN on page 96.)	
Bandwidth Throttle (See Bandwidth Throttle on page 97.)	

Keepalive

If the AirLink device does not receive a valid packet for a specified time, Keepalive tests the connection to the cellular network by pinging a configured IP address. Keepalive is only recommended if you have a remote terminated device that infrequently communicates to the network or if you have experienced issues over time where the device can no longer be reached remotely.

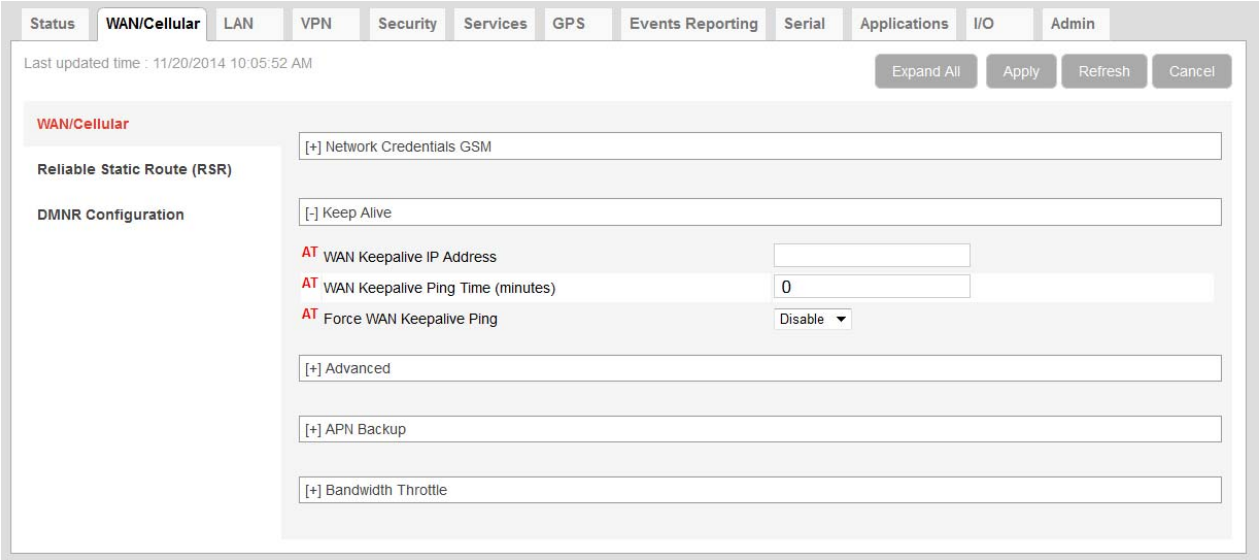


Figure 4-5: ACEmanager: Wan/Cellular > Keepalive

Field	Description
Keepalive IP Address	The IP address that the AirLink device pings to determine if there is Internet connectivity and to make sure the IP address is accessible. Enter the IP address or fully qualified domain name for the AirLink device to ping to keep itself alive (online). Options are: • IP address • Domain name You can also use *IPPINGADDR to set this parameter.

Field	Description
Keepalive Ping Time (minutes)	The amount of time the AirLink device goes without receiving a valid packet before the first Keepalive ping is sent. Options are: • 0—Disable Keepalive ping (default) • 1–255 minutes Most applications work well with an interval of 15 to 60 minutes. If the first ping fails, the AirLink device sends four additional pings. If all five pings fail, the AirLink device reboots. After rebooting, the AirLink device waits 60 minutes before sending another Keepalive ping (regardless of the setting in this field). This prevents frequent rebooting (based on the Keepalive Ping Time setting) if the IP address used for the Keepalive ping is not accessible. *Note: Using Keepalive ping may accrue data charges. Each individual ping is approximately 98 bytes (196 bytes for ping sent plus ping response).* You can also use *IPPING to set this parameter.
Force Keepalive Ping	Determines if the ping should be sent even if IP traffic is received during the Keepalive ping interval. Options are: • Disable (default) • Enable If the first ping fails, the AirLink device sends four additional pings. If all five pings fail, the AirLink device reboots. After rebooting, the AirLink device waits 60 minutes before sending another Keepalive ping (regardless of the setting in this field). This prevents frequent rebooting (based on the Keepalive Ping Time setting) if the IP address used for the Keepalive ping is not accessible. You can also use *IPPINGFORCE to configure this parameter.

SIM PIN

If you have a SIM card with a PIN configured, you can configure ALEOS to enter the PIN on reboot, so human intervention is not required.

This feature has two requirements:

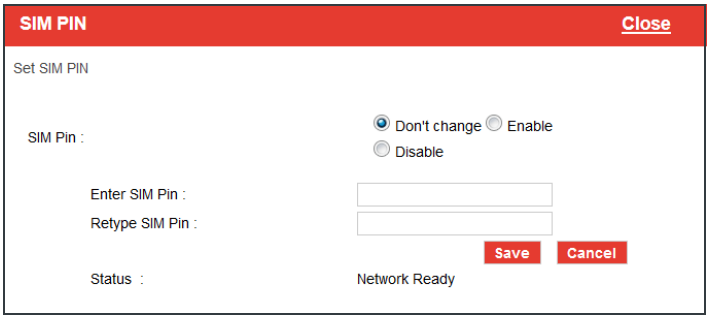
- A PIN-locked SIM card—Contact your Mobile Network Operator to ensure that they support this feature and to obtain a PIN-locked SIM card and PIN.
- The SIM PIN feature in ACEmanager must be enabled. See Enable the SIM PIN.

If the AirLink device has a PIN-locked SIM installed and this feature is not enabled in ACEmanager, the AirLink device is unable to go on air and the Network Status field on the Status > Home screen displays the message “SIM PIN incorrect, # attempts left”.

Enable the SIM PIN

To enable the SIM PIN in ALEOS:

1. In ACEmanager, go to WAN/Cellular.
2. Click the SIM PIN button. The following pop-up window appears.



3. Select Enable.
4. Enter the PIN (obtained from your Mobile Network Operator) twice and click Save.
5. Reboot the AirLink device.

After rebooting:

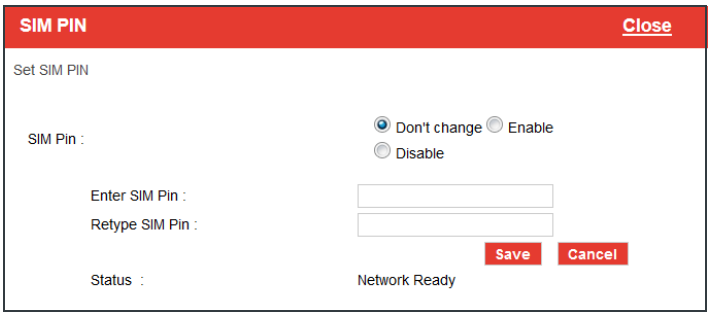
- The AirLink device uses the configured PIN on subsequent re-boots.
- The SIM PIN pop-up window shows the default settings. Don't change is selected and the SIM PIN fields are blank. "Don't change" indicates that the PIN is used in the same way on every boot.

Note: If you enter an incorrect PIN, the AirLink device is unable to go on air, and the Network Status field on the Status > Home screen displays "SIM PIN incorrect, # attempts left". The failed PIN is not retried on subsequent reboots to prevent exhausting the available number of retries with repeated attempts with an incorrect PIN.

Change the SIM PIN

To change the SIM PIN:

1. In ACEmanager, go to WAN/Cellular.
2. Click the SIM PIN button. The following pop-up window appears.



3. Select Enable.
4. Enter the new PIN twice and click Save.
5. Reboot the AirLink device.

After rebooting:

- The AirLink device uses the configured PIN on subsequent re-boots.

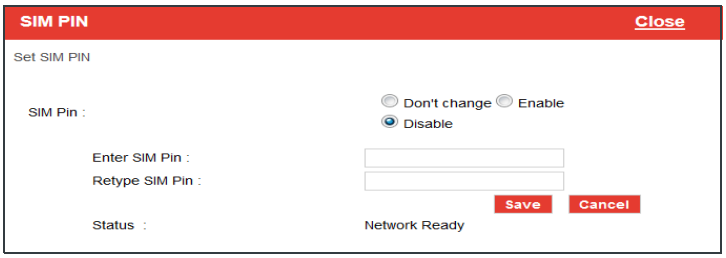
- The SIM PIN pop-up window shows the default settings. Don't change is selected and the SIM PIN fields are blank. "Don't change" indicates that the PIN is used in the same way on every boot.

Note: If you enter an incorrect PIN, the Network Status field on the Status > Home screen displays "SIM PIN incorrect, # attempts left". The failed PIN is not retried on subsequent reboots to prevent exhausting the available number of retries with repeated attempts using an incorrect PIN.

Disable the SIM PIN

To disable the SIM PIN:

1. In ACEmanager, go to WAN/Cellular.
2. Click the SIM PIN button. The following pop-up window appears.



3. Select Disable.
4. Enter the PIN twice and click Save.

   If you enter an incorrect PIN or no PIN, the feature will not be disabled.
5. Reboot the AirLink device.

After rebooting:

- The AirLink device no longer uses the stored PIN on subsequent re-boots.
- The SIM PIN pop-up window shows the shows the feature is Disabled.

Unblocking a SIM PIN

When you enable, change or disable a SIM PIN, you have a set number of attempts to enter the correct PIN, depending on your Mobile Network Operator. If the correct PIN is not entered in the alloted number of attempts, the SIM PIN becomes blocked and you need a PUK code to unblock it.

To unblock a SIM PIN:

1. Contact your Mobile Network Operator to obtain a PUK code.
2. In ACEmanager, go to WAN/Cellular.
3. Click the SIM PIN button.

   When the PIN is blocked, an additional field (Enter SIM Unblock Code) appears.
4. Enter the PUK and click Save.

Be careful when entering the PUK. You have a limited number of attempts to enter the correct PUK (generally 10) before the SIM card is disabled. If the PUK does not unblock the SIM PIN after the first few attempts, contact your Mobile Network Operator.

If you have exhausted all the alloted attempts to enter the correct PUK, the Mobile Network Operator may give you a new SIM card, or a new code to enable your existing SIM card. AirLink products do not support this type of code. To enter the code:

a. Remove the SIM card from your AirLink device (following the instructions in the AirLink Device Hardware User Guide) and insert it in a cell phone that accommodates a MiniSIM (2FF) card.

b. Enter a new code provided by the Mobile Network Operator and then return the SIM card to the AirLink device.

Re-Activation

The Re-Activation section of the WAN/Cellular tab only appears for EV-DO/1X devices. The Re-Activation feature can only be used when a particular device that has already been activated needs re-activation. If your device needs to be reactivated, click the button labeled “Re-Activate Cellular Account”. When you click this button, the status shows the progress of the re-activation.

Note: If the provision fails, an error message appears.

After the provision process finishes, the system then restarts, as a reset is necessary to initiate the new account information.

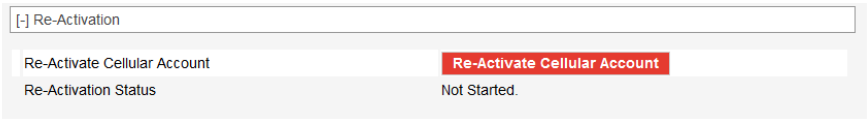


Figure 4-6: ACEmanager: WAN/Cellular > Re-Activation

Backup APN

This feature enables you to configure a backup APN to be used as a backup network connection mechanism, only if the primary APN is not available. When it is enabled, the device connects to the backup APN only if it is unable to connect to the primary APN.

Note: Switching to the backup APN can take five minutes or more, depending on the device. If the device is always connecting to the backup APN, check the primary APN to ensure that it is configured correctly.

To configure a backup APN:

1. Go to WAN/Cellular > APN Backup.

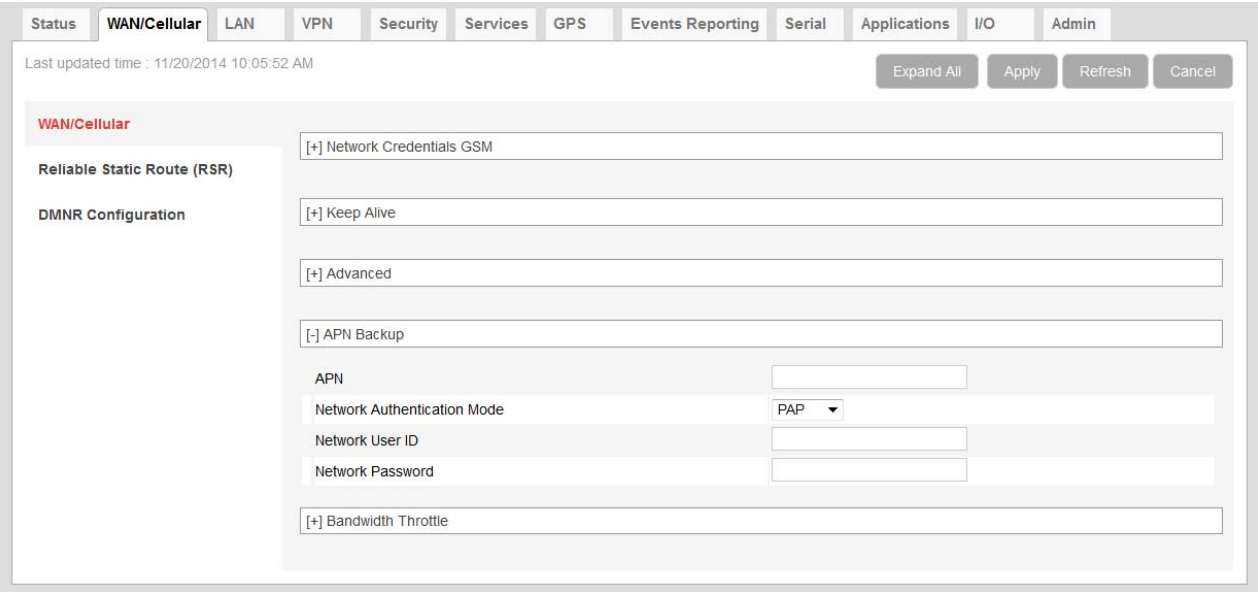


Figure 4-7: ACEmanager: WAN/Cellular > APN Backup

2. Enter the backup APN.
3. Select the Network Authentication Mode. The options are:
   - PAP (default)
   - CHAP
   - NONE
4. Enter the Network User ID and Password, if these are required for the wireless network.
5. Click Apply.

Bandwidth Throttle

This feature helps you manage your data account by allowing you to configure the AirLink device to restrict the real-time available bandwidth. You can:

- Place limits on the uplink traffic, downlink traffic, or both
- Allow for burst of traffic on the uplink, downlink, or both, while still maintaining the over-all desired bandwidth limit

Traffic that exceeds the limits is dropped. Status fields keep running tallies of data sent and received and the number of uplink and downlink packets dropped.

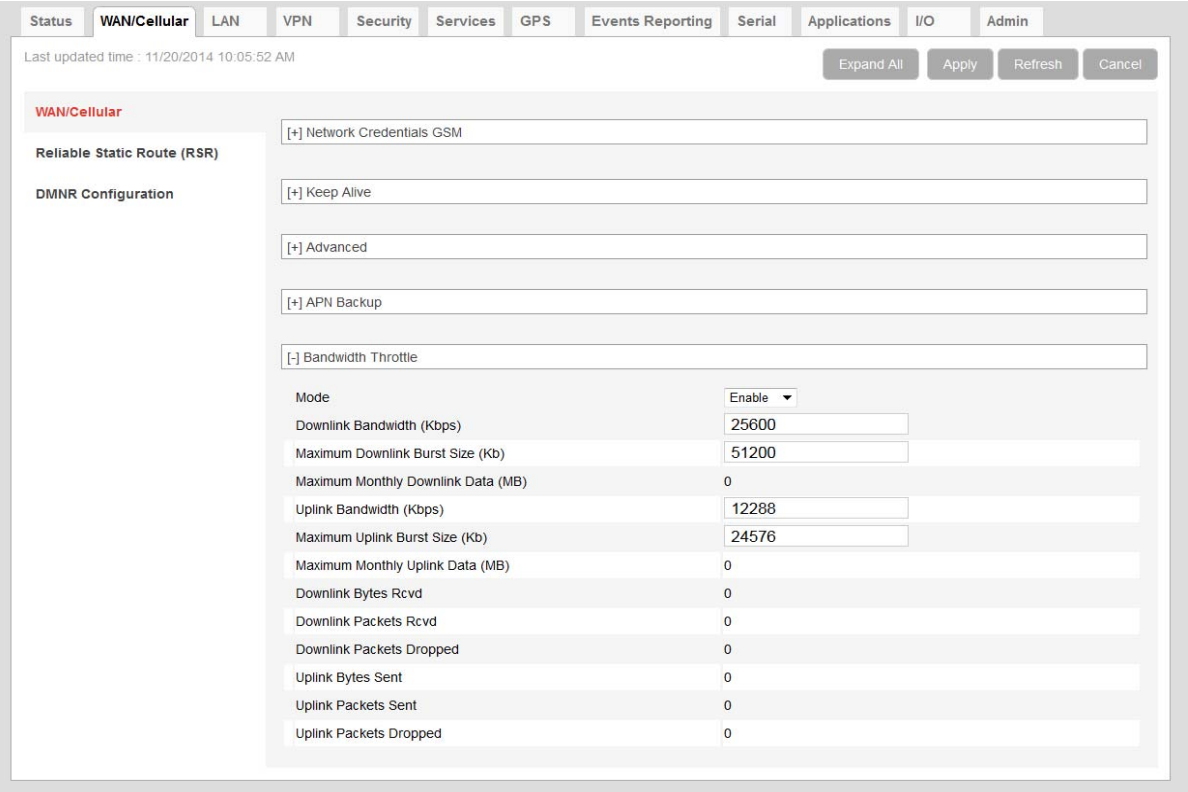


Figure 4-8: ACEmanager: WAN/Cellular > Bandwidth Throttle

Field	Description
Bandwidth Throttle	
Mode	Allows you to Enable or Disable the feature Default is Disable.
Downlink Bandwidth (Kbps)	The maximum downlink bandwidth in Kilobits per second (Kbps) This is the long-term bandwidth limit. Options are: • 0–512000 (500 Mbps) Default is 25600. 0 = feature disabled for downlink traffic

Field	Description
Maximum Downlink Burst Size (Kb)	Maximum size for bursts of downlink traffic in Kilobits (Kb) This field allows the AirLink device to handle temporary bursts of downlink traffic without dropping packets. When the actual downlink traffic is less than the value configured in the Downlink Bandwidth (Kbps) field, ALEOS collects credits that can be used for bursty traffic. The value in this field is the maximum amount of credit that can be collected. Options are: • 64–512000 (500 Mb) Default is 51200. *Note: Sierra Wireless recommends that the Maximum Downlink Burst Size be set at 2x the value configured in the Downlink Bandwidth (Kbps) field. If the Maximum Downlink Burst Size is set at more than 60x the value configured in the Downlink Bandwidth (Kbps) field, the bandwidth throttle feature is disabled for downlink traffic.*
Maximum Monthly Downlink Data (MB)	An estimate of the maximum monthly downlink data in Megabytes (MB), based on the value set in the *Downlink Bandwidth (Kbps).* Maximum monthly downlink data (MB) = Downlink bandwidth x 2592000 ÷ 8192 Where: 2592000 is the number of seconds in a month (30 days/month) 1 MB = 1024 KB; 1024 x 8 = 8192 Kb/MB
Uplink Bandwidth (Kbps)	The maximum uplink bandwidth in Kilobits per second (Kbps) This is the long-term bandwidth limit. Options are: • 0–204800 (200 Mbps) Default is 12288. 0 = feature disabled for uplink traffic
Maximum Uplink Burst Size (Kb)	Maximum size for bursts of uplink traffic in Kilobits (Kb) This field allows the AirLink device to handle temporary bursts of uplink traffic without dropping packets. When the actual uplink traffic is less than the value configured in the Uplink Bandwidth (Kbps) field, ALEOS collects credits that can be used for bursty traffic. The value in this field is the maximum amount of credit that can be collected. Options are: • 32–204800 (200 Mb) Default is 24576. *Note: Sierra Wireless recommends that the Maximum Uplink Burst Size be set at 2x the value configured in the Uplink Bandwidth (Kbps) field. If the Maximum Uplink Burst Size is set at more than 60x the value configured in the Uplink Bandwidth (Kbps) field, the bandwidth throttle feature is disabled for uplink traffic.*
Maximum Monthly Uplink Data (MB)	An estimate of the maximum monthly uplink data i in Megabytes (MB), based on the value set in the *Uplink Bandwidth (Kbps)* Maximum monthly uplink data (MB) = Uplink bandwidth x 2592000 ÷ 8192 Where: 2592000 is the number of seconds in a month (30 days/month) 1 MB = 1024 KB; 1024 x 8 = 8192 Kb/MB
Downlink Bytes Rcvd	Number of downlink bytes received The value is updated every 30 seconds, and is reset to zero on device reboot or reset to factory default settings.

Field	Description
Downlink Packets Rcvd	Number of downlink packets received The value is updated every 30 seconds, and is reset to zero on device reboot or reset to factory default settings.
Downlink Packets Dropped	Number of downlink packets dropped because the limits set in Downlink Bandwidth (Kbps) and Maximum Downlink Burst Size (Kb) have been exceeded The value is updated every 30 seconds, and is reset to zero on device reboot or reset to factory default settings.
Uplink Bytes Sent	Number of uplink bytes sent The value is updated every 30 seconds, and is reset to zero on device reboot or reset to factory default settings.
Uplink Packets Sent	Number of uplink packets sent The value is updated every 30 seconds, and is reset to zero on device reboot or reset to factory default settings.
Uplink Packets Dropped	Number of uplink packets dropped because the limits set in Uplink Bandwidth (Kbps) and Maximum Uplink Burst Size (Kb) have been exceeded The value is updated every 30 seconds, and is reset to zero on device reboot or reset to factory default settings.

Reliable Static Routing (RSR)

Reliable Static Routing enables you to force specified traffic to use different routing rules (rather than the default, which is usually cellular) to direct specified traffic (from or to either the AirLink device or a connected device) to a designated primary route. If the primary route fails, the specified traffic uses a backup route.

First, you designate specific traffic to use the primary route, based on the destination IP address and subnet mask. A configured Tracking Object Test verifies the validity of the primary route. If the test fails, the backup route is used. The Tracking Object Test continues to run and as soon as it returns a “Pass”, traffic is switched back to the primary route.

You can direct the traffic to a network (Figure 4-9) or to an individual host (Figure 4-10).

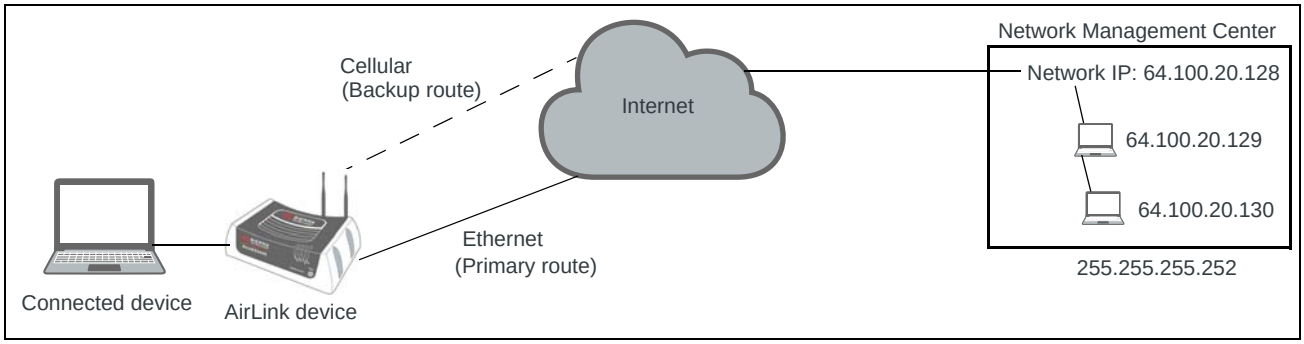


Figure 4-9: RSR directed to a destination network

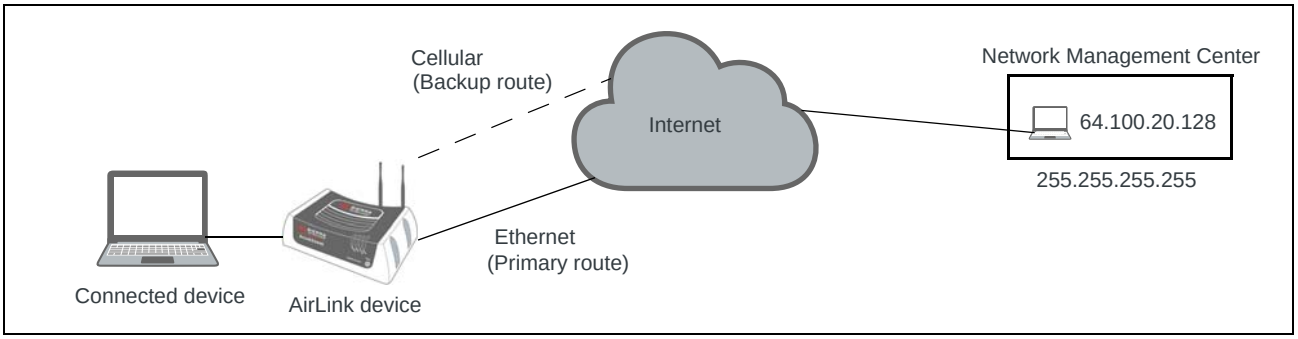


Figure 4-10: RSR directed to a destination IP address (individual host)

In a business continuity application where the router also has a routable IP address from a wireline gateway connection (as shown in Figure 4-11) the IT administrator may prefer to use that lower cost connection for data sourced from the AirLink device, such as SNMP or AVMS data. When reliable static routing is configured, the Tracking Object tests the validity of the primary route and data from the AirLink device is transmitted through the primary route (in this example, the wireline connection). If the tracking object determines that the primary route is down, data is transmitted through the backup (in this example, the wireless connection).

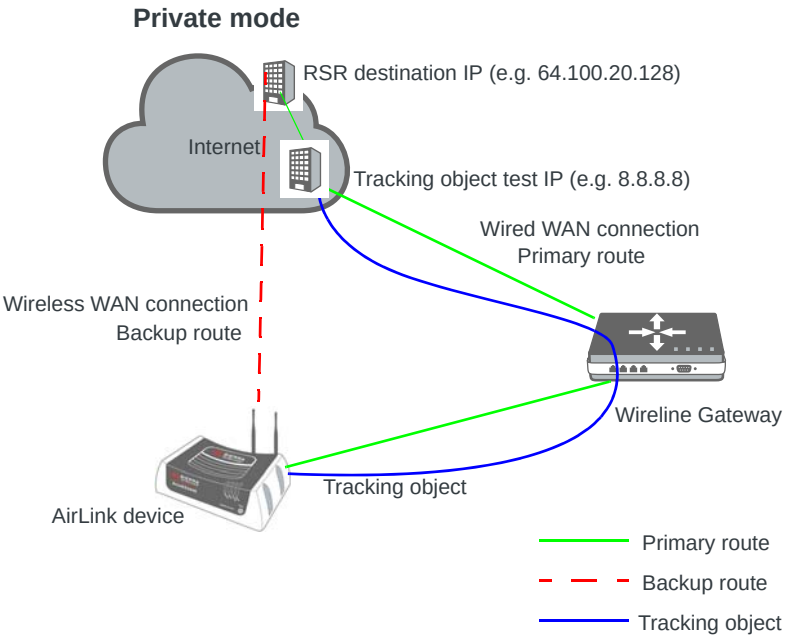


Figure 4-11: Private Mode with Reliable Static Routing

Sierra Wireless recommends a Private Mode network as the most reliable configuration to use in a business continuity failover application as defined in the AirLink Hardware User Guide (or Figure 4-11) with Reliable Static Routing and Reverse Telnet. For more information, see Private and Public Mode on page 111.

To configure Reliable Static Routing:

1. Connect the hardware as shown in Figure 4-11.

2. Use the Tracking Object to test the connection:
   a. In ACEmanager, go to WAN/Cellular > Reliable Static Route (RSR).

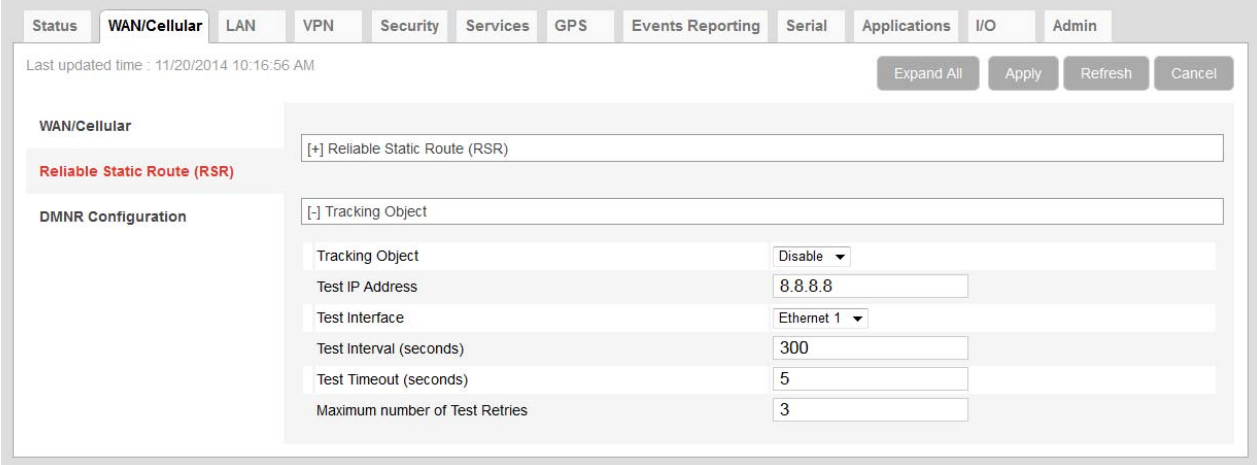


Figure 4-12: ACEmanager: WAN/Cellular > Reliable Static Route (RSR), Tracking Object

   b. Under Tracking Object, enter the Test IP address, using a host behind the gateway that has a reliable IP address, such as 8.8.8.8.
   c. From the drop-down menu, select Ethernet 1 as the Test Interface.
   d. Leave the default values for the Test Interval, Test Timeout, and Maximum number of retries.
   e. In the Enable/Disable Tracking Object field, select Enable.
   f. Click Apply.
   g. The Tracking Object pings the Test IP address configured in step b. In ACEmanager go to Status > WAN/Cellular and note the result in the RSR Test Result field.
3. Disable Tracking Object.

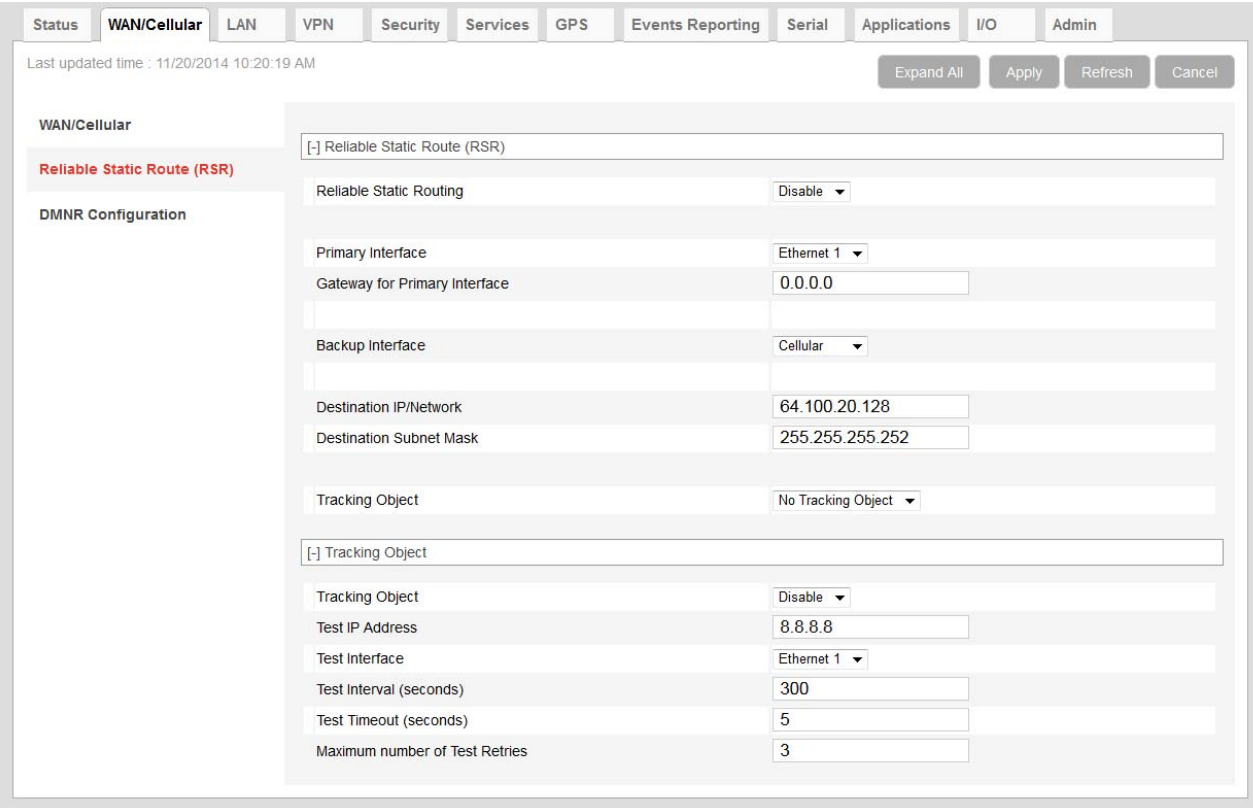


Figure 4-13: ACEmanager: WAN/Cellular > Reliable Static Route (RSR)

Note: Configure all the other fields before setting the Enable/Disable Reliable Static Routing field. Once you enable RSR, some fields on this page are not editable.

4. Select the interfaces for the primary and backup routes. The options are:

- Ethernet 1 (default for primary route) If you are using a GX Series device with a Dual Ethernet X-Card installed, the additional Ethernet ports will appear in the drop-down menu as Ethernet 2 and Ethernet 3.
- USB
- Wi-Fi (Available only if you have a GX Series device with a Wi-Fi X-Card installed)
- Cellular (default for backup route)

If you select Ethernet 1, you are given the option to enter a gateway IP address that is used as the next hop for reaching the destination network.[1]

- If the Tracking Object test completed in step 2 was successful, leave this field at the default value (0.0.0.0).

1. This applies to both the Primary and the Backup interface.

- If the Tracking Object test completed in step 2 failed, enter the gateway IP address in this field.

5. Set the Destination IP/Network and Destination Subnet Mask.

   To configure the RSR destination as a network, as shown in Figure 4-13, you would enter:
   - 64.100.20.128 in the Destination IP/Network field.
   - 255.255.255.252 in the Destination Subnet Mask field.

   To configure the RSR destination as an individual host, as shown in Figure 4-13, you would enter:
   - 64.100.20.128 in the Destination IP/Network field.
   - 255.255.255.255 in the Destination Subnet Mask field.
6. Set the Tracking Object (Tracking Object 1 or No Tracking Object). Normally, you would select Tracking Object 1 from the drop-down menu.
7. Under Tracking Object, leave the Enable/Disable Tracking Object set at Disable until you finish configuring the other Tracking Object fields.
8. Enter the Test IP address (normally an IP address within the Traffic Selection Criteria Network/Subnet).
9. From the drop-down menu, select the desired Test Interface (normally the same interface as the primary route). Options are:
   - Ethernet 1 (If you are using a GX Series device with a Dual Ethernet X-Card installed, the additional Ethernet ports will appear in the drop-down menu as Ethernet 2 and Ethernet 3.)
   - USB
   - Wi-Fi (Available only if you have a GX Series device with a Wi-Fi X-Card installed)
   - Cellular
10. Enter the Test Interval in seconds. This is the interval between Tracking Object Tests.

    For most applications, the default values for the Test Interval, Test Timeout, and Maximum number of retries should be fine.

    If you want to change these values, be aware of the following:
    - Selecting a short test interval increases network traffic and may lead to false failures if the network is busy.
    - Selecting a long test interval may mean that traffic does not switch to the secondary route quickly enough when the primary route fails.
    - The test interval must be greater than the product of Test Timeout x Maximum number of Test Retries.
      [Test Interval] > [Test Timeout] x [Maximum number of Retries]
11. Enter the Test Timeout in seconds. This is the time to wait for a response. If this time expires before a response is received, the test attempt fails.
12. Enter the Maximum number of Test Retries. If the first Tracking Object Test fails, this is the number of times the device sends additional test messages (without receiving a response) before it declares the test as failed and switches the specified traffic to the backup network.
13. In the Enable/Disable Tracking Object field, select Enable.
14. In the Enable/Disable RSR field, select Enable.

Go to Status > WAN/Cellular to check the RSR Test Result and confirm that traffic is being sent through the primary route. If the RSR Test Result field indicated that the Tracking Object Test has failed, validate the connectivity of the primary path. (The test result of Unknown indicates that the test has not yet run.)

Dynamic Mobile Network Routing (DMNR)

Note: DMNR is supported only on the Verizon Wireless network.

DMNR provides direct communication between customer sites (for example, between remote subnets and the corporate data center) through a Mobile Network Operator's (MNO's) private network (isolated from Internet traffic).

DMNR creates a tunnel between the home agent on the MNO's private network and the AirLink device.

Note: Primary Access Mode DMNR is supported on Ethernet LANs. DMNR is not supported on Wi-Fi bridged to Ethernet (Bridge Wi-Fi to Ethernet).

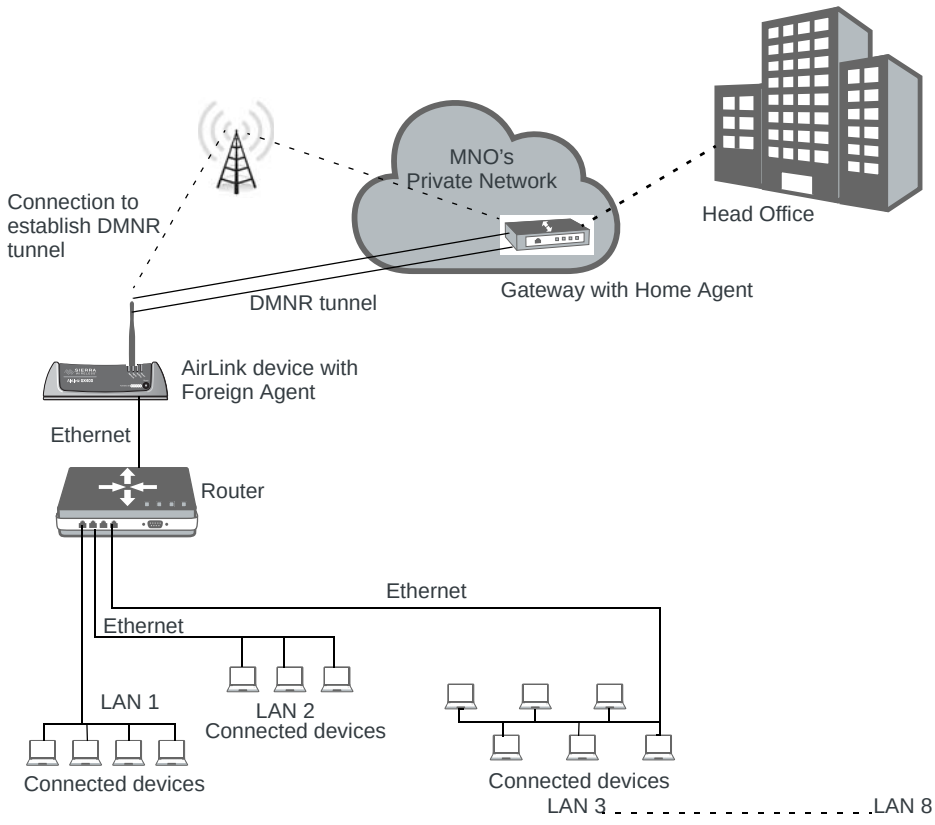


Figure 4-14: DMNR Configuration

Before configuring DMNR:

1. Go to LAN > DHCP/Addressing and ensure that the Host Connection Mode is set to All Hosts Use Private IPs (default).
2. Go to VPN and disable any VPNs you have set up.

   Once DMNR is configured, all traffic from the connected LANs goes through the DMNR tunnel.

To configure DMNR:

1. Go to WAN/Cellular > DMNR Configuration.

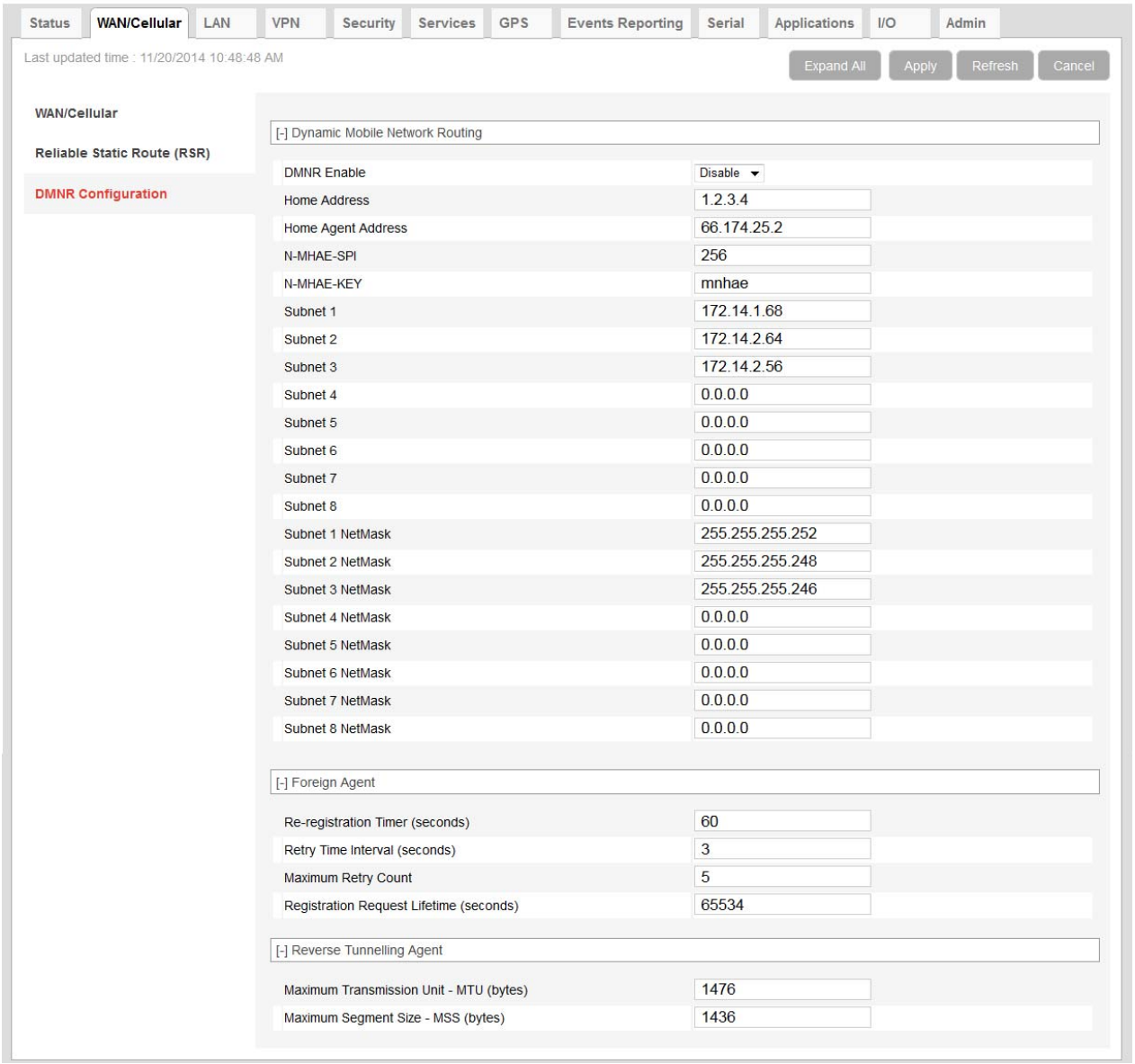


Figure 4-15: ACEmanager: WAN/Cellular > DMNR Configuration

2. Configure the fields as outlined in the following table.

Field	Description
Dynamic Mobile Network Routing	
DMNR Enable	Enables Dynamic Mobile Network Routing. Options are: • Enable • Disable (default) *Note: Configure all the other parameters first and then set this field to Enable. When this field is set to Enable, the other fields in this window are read-only.*
Home Address	Enter a home address for the AirLink device. This address is used to distinguish the AirLink device used for DMNR. You can enter any IP address for the Home Address, but if you are using more than one AirLink device for DMNR, each must have a different home address. Suggested value is 1.2.3.4. This field cannot be left blank.
Home Agent Address	IP address of the Home Agent (available from your Mobile Network Operator)
N-MHAE-SPI	NEMO Authentication Extension Security Parameter Index (available from your Mobile Network Operator)
N-MHAE-KEY	NEMO Authentication Extension Key (available from your Mobile Network Operator)
Subnet 1 – 8	Enter the IP addresses for the subnets you want to include in the DMNR network. You can configure up to 8 subnets. 0.0.0.0 indicates that the subnet is not configured. *Note: If you want to remove a subnet from the DMNR configuration, replace the IP address with 0.0.0.0 rather than deleting it.*
Subnet 1 – 8 NetMask	Enter the Subnet Masks for the subnets you want to include in the DMNR network. 0.0.0.0 indicates that the subnet mask is not configured. *Note: If you want to remove a subnet mask from the DMNR configuration, replace the IP address with 0.0.0.0 rather than deleting it.*

3. Click the + beside Foreign Agent and Reverse Tunnelling Agent.

4. Configure the Foreign Agent and Reverse Tunnelling Agent.

Field	Description
Foreign Agent	
Re-registration Timer (seconds)	The frequency with which the foreign agent re-registers its subnets • If the registration status is Down, the foreign agent re-registers its subnets when the time configured in this field expires. • If the registration status is Up, the frequency with which the foreign agent re-registers its subnets is equal to the Registration Response Lifetime minus the value configured in this field. The Registration Response Lifetime is usually equal to the Registration Request Lifetime (seconds). Once you have enabled DMNR, you can confirm the Registration Response Lifetime in ACEmanager (see Figure 4-16 on page 109). Options are: • 1–60 seconds (Default is 60 seconds.)
Retry Time Interval (seconds)	The interval (in seconds) between retries if the re-registration fails. Options are: • 1–5 seconds (Default is 5 seconds.)
Maximum Retry Count	Maximum number of re-registration tries allowed. Options are: • 0–5 (Default is 3.)
Registration Request Lifetime (seconds)	Enter the desired registration lease time (in seconds). Options are: • 0–65534 seconds (Default is 65534.)
Reverse Tunneling Agent	
Maximum Transmission Unit - MTU (bytes)	Use this field to set the Maximum Transmit Unit for packets sent over the DMNR/GRE tunnel. Note that the tunnel adds 24 bytes to each packet so the MTU should be set such that MTU + 24 is less than the mobile network MTU. Otherwise packet fragmentation may occur. Options are: • 576–1500 (Default is 1476.)
Maximum Segment Size - MSS (bytes)	Use this field to set the maximum segment size for the packets (in bytes). Options are: • 68–1436 (Default is 1436.)

5. In the DMNR Enable field, select Enable.

   Once DMNR is enabled, the fields are read-only. If you want to change any of the field entries, set the DMNR Enable field to Disable, make the required change, and then set the field to Enable.

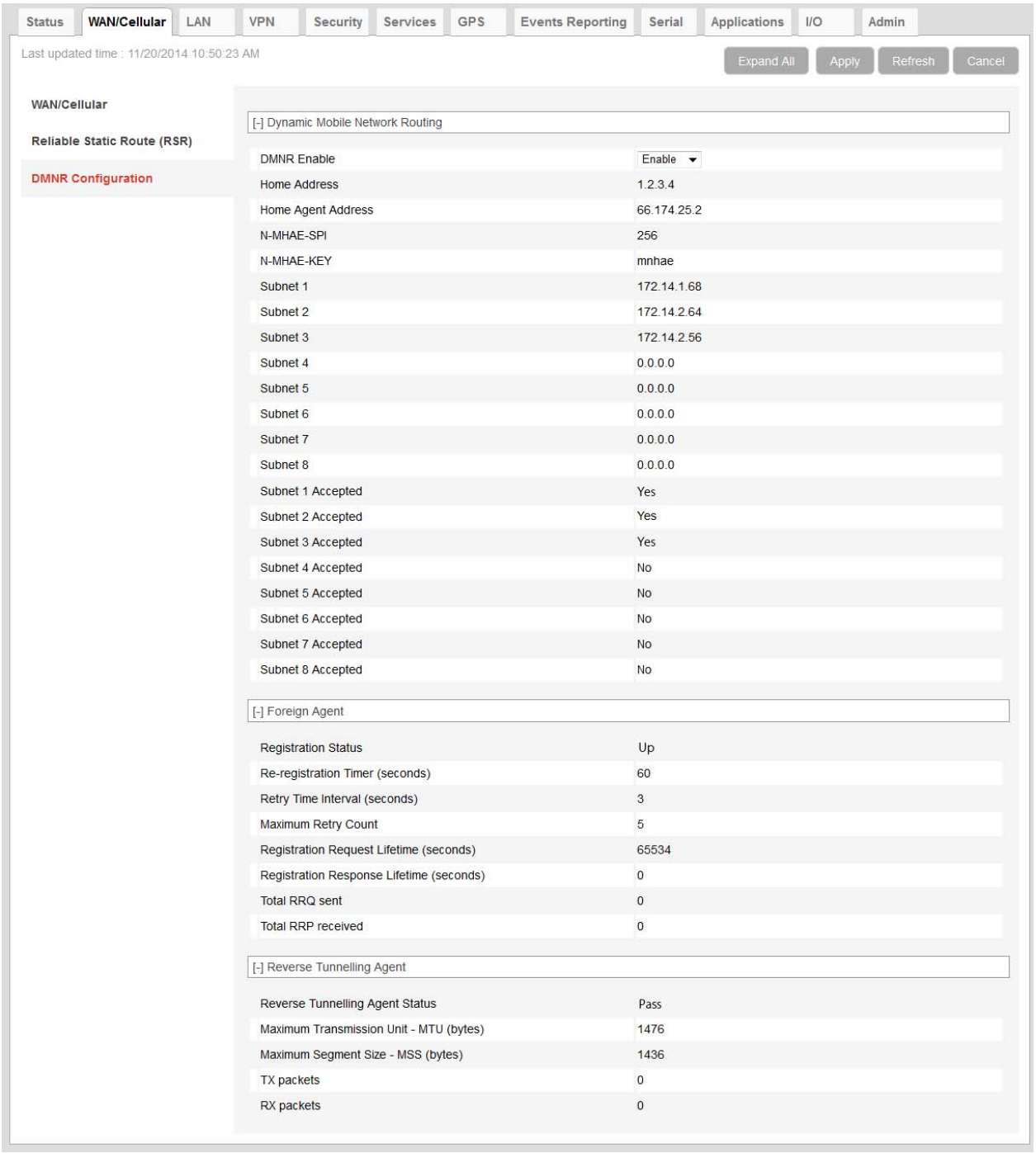


Figure 4-16: ACEmanager: WAN/Cellular > DMNR Enabled

Once DMNR is enabled, additional status fields appear, as described in the following table.

Field	Description
Dynamic Mobile Network Routing	
Subnet 1–8 Accepted	Confirms that the subnet configuration is accepted. Options displayed are: Yes, No. If the subnet is not configured, No appears in this field.
Foreign Agent	
Registration Status	Foreign agent registration status Options displayed are: Pass, Fail, or Unknown *Note: If the Ethernet cable between the AirLink device and the router (see Figure 4-14 on page 105) is disconnected, the Registration Status continues to show "Pass", but the Reverse Tunnelling Agent Status is shown as "Down", and subnets appear as not accepted.*
Registration Response Lifetime (seconds)	Shows the length of the current lease time (in seconds).
Total RRQ sent	Number of Registration Requests sent
Total RRP received	Number of Registration Responses received
Reverse Tunneling Agent	
Reverse Tunnelling Agent Status	Reverse tunnelling agent status This field only appears when DMNR is enabled. Options displayed are: Up, Down.
TX packets	Number of packets transmitted The counter is reset when: • DMNR is disabled. • The radio network status changes from Ready to Not in service.
RX packets	Number of packets received The counter is reset when: • DMNR is disabled. • The radio network status changes from Ready to Not in service.

5: LAN/Wi-Fi Configuration

5

Note: The LAN/Wi-Fi tab in ACEmanager only appears when a Wi-Fi X-Card is installed in the AirLink GX Series device. If a Wi-Fi X-Card is not installed, this tab appears as LAN.

You can use the AirLink device to route data between one or more connected devices and the Internet via the mobile network. The AirLink device has two modes you can use for configuring a LAN—Private Mode and Public Mode.

Private and Public Mode

Private Mode and Public Mode are Sierra Wireless terms. In Private Mode, the router or laptop connected to the AirLink device has a LAN IP address. In Public Mode the AirLink device passes the WAN IP address to the router or laptop. Figure 5-1 shows the two types of configurations.

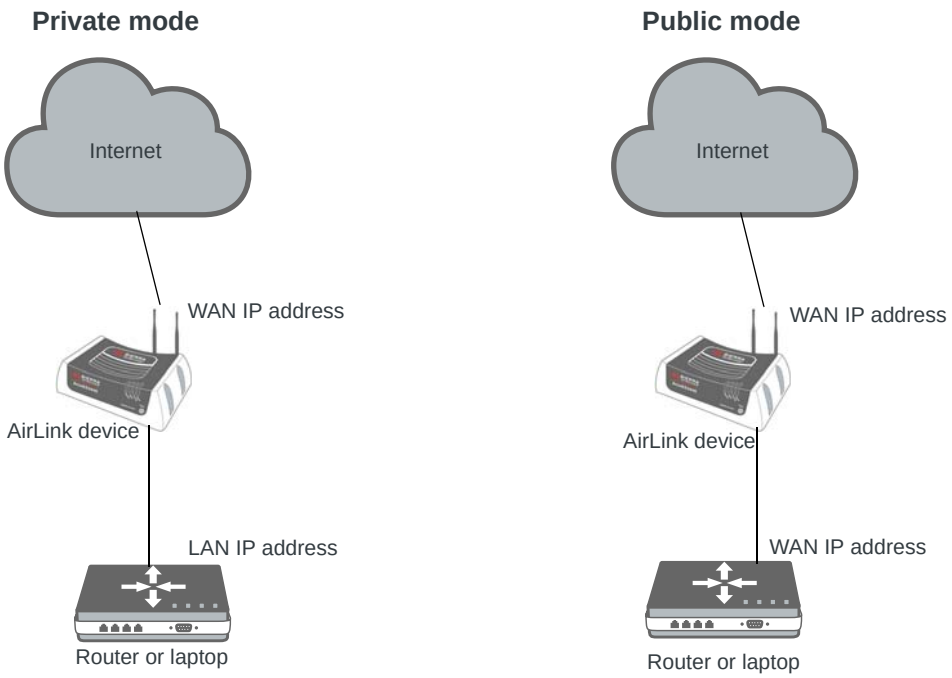


Figure 5-1: Private vs. Public Mode

Private Mode

Private Mode uses Network Address Translation (NAT) to enable the non-routable device to access the Internet. Data from the connected devices is passed through the AirLink device. By default, the first connected Ethernet or USBnet host is the DMZ host.

Public Mode

Public Mode is similar to IP pass-through. When Public Mode is enabled, by default the Public Mode host becomes the DMZ host. Public Mode is required when the connected device needs a routable IP address and has no other connection to obtain it.

Tip: *When using Public Mode, Sierra Wireless recommends connecting the AirLink device directly to the computer or other end device. Using a hub or switch may prevent the AirLink device from updating the IP address of the end device when an IP address is received from the cellular network.*

Port Use

Applications running on a LAN client such as a router or laptop must use different ports from those used by ALEOS features on the AirLink device. For a list of inbound ports used by ALEOS, see Inbound Ports Used by ALEOS on page 466.

DHCP/Addressing

This section is primarily a status display of the configurations, with a few options that are global to all interface types. Interfaces that are enabled in the current configuration are displayed with their configured settings.

DHCP addresses and subnets are assigned to the LAN side interfaces display. If no Wi-Fi X-Card is installed in an AirLink GX Series device, select the DHCP/Addressing section from the LAN tab to display a screen similar to the Figure 5-1 example.

Note: If the device has not been reset since configuration changes were made, the current configuration in use may be different.

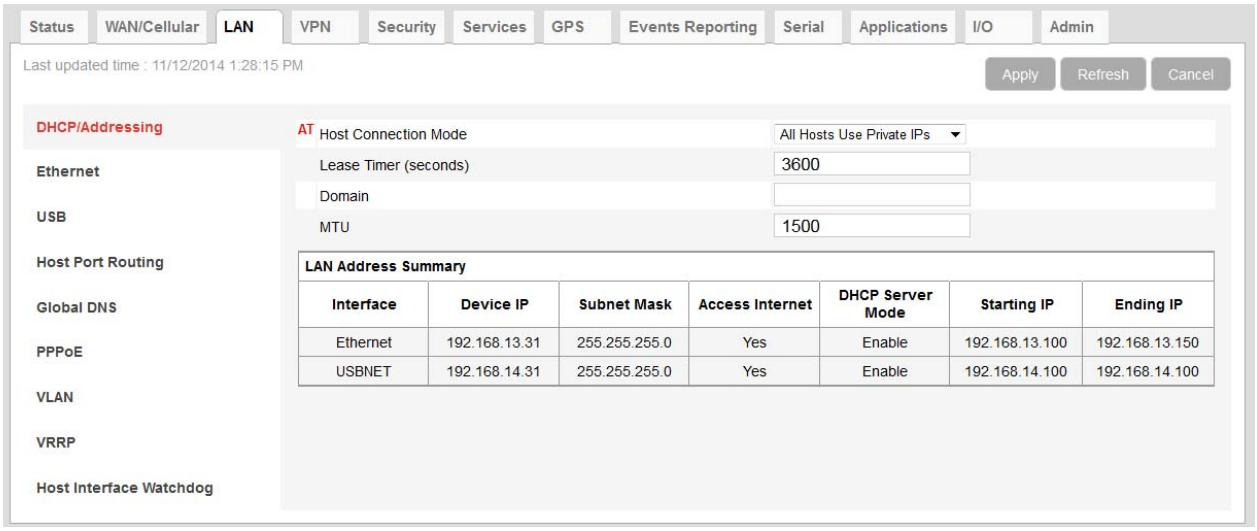


Figure 5-2: ACEmanager: LAN/Wi-Fi > DHCP/Addressing

If a Wi-Fi X-Card is installed in the AirLink GX Series device, the LAN tab changes to LAN/Wi-Fi, and selecting DHCP/Addressing displays a screen similar to Figure 5-2. When Wi-Fi is bridged to Ethernet, the Bridge Wi-Fi to Ethernet field displays Enabled, and Ethernet and Wi-Fi appear in the same subnet row.

Note: Bridging between Wi-Fi and USB/net is not supported.

Field	Description
Host Connection Mode	Sets the Host Interface to use the Public IP address granted by the cellular network or private IP addresses. All host interfaces which are not using the public IP address use private IP addresses. The options are: • Ethernet Uses Public IP* • All Hosts Use Private IP—(default) • USB Uses Public IP • Serial DUN Uses Public IP • First Host gets Public IP If you select this option, you do not have to specify the type of connection that uses the Public IP address. The first device to connect uses the Public IP address, regardless of whether it has a USB or Ethernet connection.* For more information on Private and Public mode, see Private and Public Mode on page 111. *Note: If you plan on using Dynamic Mobile Network Routing (DMNR) on page 105, select Ethernet Uses Public IP in this field.* **Caution:** ** If the AirLink GX Series device has a Dual Ethernet X-Card installed, selecting this option disables the additional Ethernet ports on the Dual Ethernet X-Card. The main Ethernet port is still functional.* *Note: The connected computer receives the DHCP address from ALEOS and it also provides a static route (192.168.13.31 by default) that allows you to access ACEmanager from a connected device.*
Public Mode Subnet Mask	This field appears when Ethernet, USB, or Serial (RS232) Uses Public IP is selected in the Host Connection Mode field. Public Mode subnet mask indicates the range of Public Mode host IP addresses. Options are: • 255.255.255.0 (24-bit) (default) • 255.255.255.255 (32-bit) Choose the option that matches the subnet mask received from the mobile network.
Lease Timer (seconds)	The amount of time the DHCP client is given for the use of the IP address (in seconds) Options are: • 120–4294967295—Number of seconds the IP address is leased for. If you want to set the value to “infinity”, enter 4294967295 (equivalent to 136 years). The actual maximum value depends on the maximum supported by your DHCP client. The default lease time is 3600 seconds (1 hour).
Domain	Displays the DHCP domain name This domain name is passed to the DHCP host in option 15 of the DHCP packet.
MTU	Sets the maximum transmission unit size The maximum transmission unit size is sent to the DHCP host in option 26 of the DHCP packet. The default is 1500.

Field	Description
Bridge Wi-Fi to Ethernet	Allows routing between the Ethernet LAN and Wi-Fi. When enabled, the Ethernet port and the Wi-Fi ports are on the same subnet. Options are: • Enabled (default) • Disabled This field is only available when on a GX Series device with a Wi-Fi X-Card is installed.
Wi-Fi Mode	Indicates the Wi-Fi module mode This field is only available when a Wi-Fi X-card is installed.
WAN IP Address	Displays the WAN IP address when the Wi-Fi is used in client mode for WAN connectivity
LAN Address Summary	Displays the interfaces which have been enabled. By default, only the Ethernet and USBNET Interfaces are enabled.
Interface	The physical interface port or VLAN ID
Device IP	The IP address of the AirLink device for the specified interface port. By default, this is set to 192.168.13.31 for Ethernet/Wi-Fi and 192.168.14.31 for USB/net.
Subnet Mask	Subnet mask indicates the range of host IP addresses that can be reached directly. Changing this limits or expands the number of clients that can connect to the AirLink device. The default of 255.255.255.0 means that 254 clients can connect to the AirLink device. Uses 192.168.13. as the first three octets of the IP address if the device IP is 192.168.13.31.
Access Internet	Appears if the interface is configured to allow connected host(s) access to the Internet *Note: Internet access cannot be disabled for Ethernet or Wi-Fi hosts.*
DHCP Server Mode	Indicates whether or not the interface has a DHCP server enabled to provide dynamically allocated IP addresses provided to connected hosts
Starting IP	Ethernet DHCP pool starting IP address
Ending IP	The ending IP for the interface. If the starting and ending IP are the same, there is a single address in the pool and only one host receives an IP address from the DHCP server for that interface. Some interfaces, such as USB, can only have a single host connection. For others, statically assigned IP addresses in the same subnet, but outside of the DHCP pool, can still connect and use the device in the same way as a DHCP connected host.

Tip: *If you are using Private Mode for all hosts (*HOSTPRIVMODE=1), make sure that device IP, Starting IP, and Ending IP are on the same subnet defined by the DHCP network mask. If the subnet mask is 255.255.255.0, it is safe to use 192.168.x.y for each as long as the x is the same number (0 in the example screen shot above) and the y is different (1 and 2 in the example) and between 0 and 254.*

Internal DHCP Server

DHCP (Dynamic Host Configuration Protocol) has become a primary component of today's network environments. DHCP allows one server to automatically and dynamically allocate network IP addresses and other network related settings

(such as subnet masks, routers, etc.) to each computer or device without the need to set up each specifically or keep track of what addresses have already been used.

In a default configuration, the AirLink device acts as a DHCP host to any device connected to its ports. This DHCP host provides that device with an IP address that can be used to communicate on the Internet.

Address Assignment in Public Mode

1. When the AirLink device registers on the cellular network, it is assigned an IP address from the carrier, e.g., 10.1.2.0.
2. When using a specific interface, the AirLink device acts as a DHCP server unless disabled. When the Host Connection Mode is Ethernet Uses Public IP, and the AirLink device receives a DHCP request from an Ethernet device connected to its ports, it hands off the assigned address to the device and sets up the default gateway address as 10.1.2.1. If the fourth octet value is already a 1, it assigns 10.1.2.2 as the router address.

Note: The primary gateway to the cellular network, for any connected device, is enabled by default.

3. The AirLink device also sends a /24 netmask (255.255.255.0 by default) and sets up a static route which maps 192.168.13.31 (or the address configured with *HOSTPEERIP if it is changed) to 10.1.2.1 (or 10.1.2.2 if that was what the gateway address was given as).

Tip: *When PPPoE is used with the AirLink device, the DHCP server needs to be disabled. A tunnel is set up connecting a device (such as your computer or a router) with the AirLink device. The device then uses the MAC address of the AirLink device to send all outgoing packets.*

Ethernet

The AirLink device is equipped with an Ethernet port that can be enabled or disabled as needed. When the port is disabled, the host cannot connect via Ethernet, and ARP queries do not receive responses on the port.

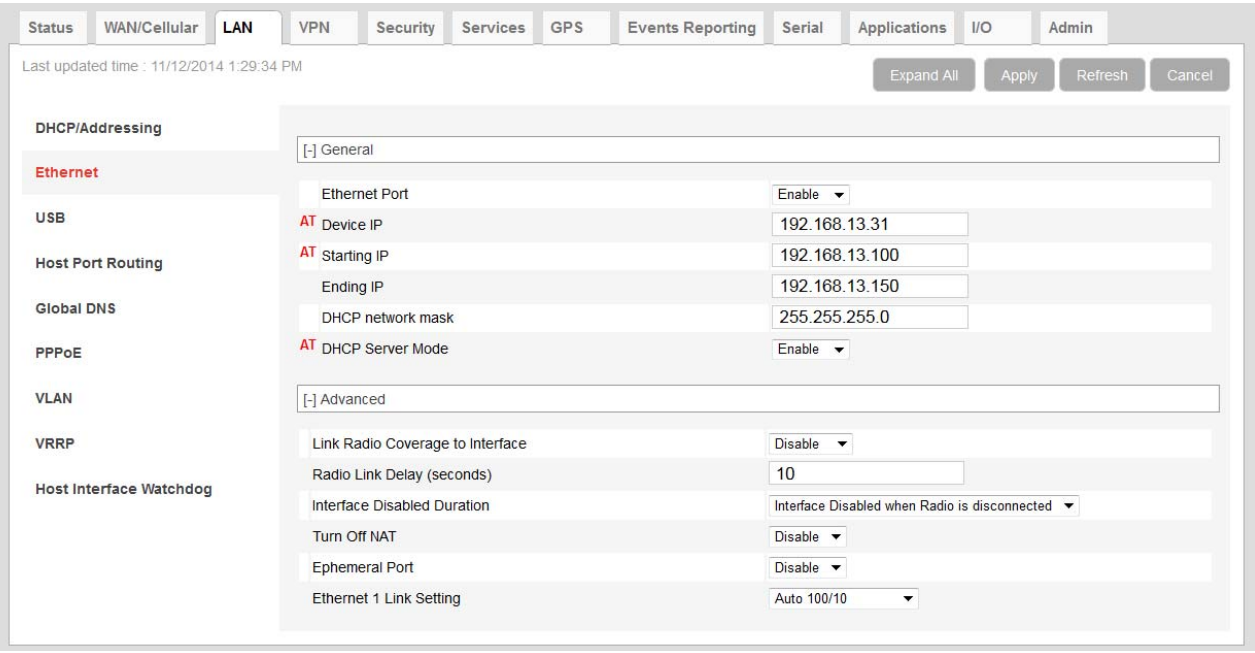


Figure 5-3: ACEmanager: LAN > Ethernet

Field	Description
General	
Ethernet Port	Enabled or Disabled *Note: When the port is disabled, the device ignores any physical connection to the Ethernet port.*
Device IP	The Ethernet IP address of the AirLink device. By default this is set to 192.168.13.31.
Starting IP	Ethernet DHCP pool starting IP address *Note: If only one computer or device is connected directly to the Ethernet port, this is the IP address it is assigned.*
Ending IP	The ending IP address for the Ethernet interface DHCP pool
DHCP network mask	The Netmask given to any Ethernet DHCP client

Field	Description
DHCP Server Mode	Enabled or disabled. By default, the Ethernet DHCP server is enabled. Disabling the DHCP server requires all connected clients to have static IP addressing. Static IP hosts need to be within the same subnet as defined by the device IP and DHCP network mask.
Advanced	
Link Radio coverage to Interface	This disables the specified port when there is no cellular coverage. Options are: • Disable (default) • Ethernet • USB
Radio Link Delay (seconds)	The delay in seconds before the selected interface goes down when there is no cellular coverage
Interface Disabled Duration	Sets the period of time (in seconds) that the LAN interface is disabled when linking a LAN port to radio coverage. Either the Ethernet or the USB LAN port can be linked to the radio coverage, but not at the same time. Options are: • Interface Disabled when Radio is disconnected (default) • 5 Sec • 10 Sec • 15 Sec • 20 Sec • 25 Sec • 30 Sec
Turn Off NAT	When enabled, ALEOS routes packets without performing NAT on them. Options: Disabled (default) and Enabled.
Ephemeral Port	Enable or Disable the Ephemeral Port feature • Disable—The source port in packets the AirLink device receives from a host device and then sends out is not changed. The source port assigned to the packet when it was created in the customer's host device is used. (default) • Enable—The AirLink device changes the source port on all outgoing NATed UDP packets, using the range configured in the Starting Ephemeral Port field.

Field	Description
Starting Ephemeral Port	This field appears only when the Ephemeral Port field is set to Enable. It allows you to set the starting port range used by a LAN host as the source port for over-the-air (OTA) destinations using NAT. *Note: This field is intended for advanced users only. In most cases, use the default value.* The NAT for the LAN host uses a range of 1000 ports as source ports for OTA destinations beginning with the configured Ephemeral port. Options are: • 1024 (default)–64535 If you have a network with multiple LAN hosts that are sending data to the same server and the server is not receiving data from one (or more) of the hosts, it may be because the Mobile Network Operator has a WAN firewall that is blocking the ports used by the NAT for over-the-air (OTA) destinations. This field enables you to avoid the blocked ports by changing the source port range used to send the data. For example, some users have found that changing the starting port to 42000 has resolved the issue. *Note: The ephemeral port setting does not affect any outbound traffic initiated by the device such as GPS reports, serial PAD or Modbus, Events Reporting, Device Initiated AVMS connection, etc.*
Ethernet 1 Link Setting **Ethernet 2 Link Setting** **Ethernet 3 Link Setting**	Configures the Ethernet port speed and duplex setting Most of the time you can leave the default setting and the device you are connecting automatically negotiates the speed and duplex setting with the AirLink device. However, if the connected device has a fixed setting, use this field to change the AirLink device setting to match that of the connected device. The options are: • Auto 100/10 (default) • Auto 10 Mb only • 100 Mb Full Duplex • 100 Mb Half Duplex • 10 Mb Full Duplex • 10 Mb Half Duplex If you have a GX Series device with a Dual Ethernet X-Card installed, ACEmanager displays separate fields for each Ethernet port. You can view the current speed and duplex setting on the Status > LAN page. See page 62.

USB

The AirLink device is equipped with a USB port that increases the methods by which you can send and receive data from a connected computer. You can set up the USB port to work as either a virtual Ethernet port or a virtual serial port, or you can disable it to prevent access by USB. A driver installation is required to use the USB port in either mode.

By default, the port is set to work as a virtual Ethernet port.

Note: Sierra Wireless recommends that you use a USB 2.0 cable with your AirLink device and connect directly to your computer for best throughput.

To change the USB port to allow virtual serial port communication:

1. In ACEmanager, go to LAN > USB, and choose USB Serial as the USB Device Mode.

   To disable the USB port, select Disable from the same menu.

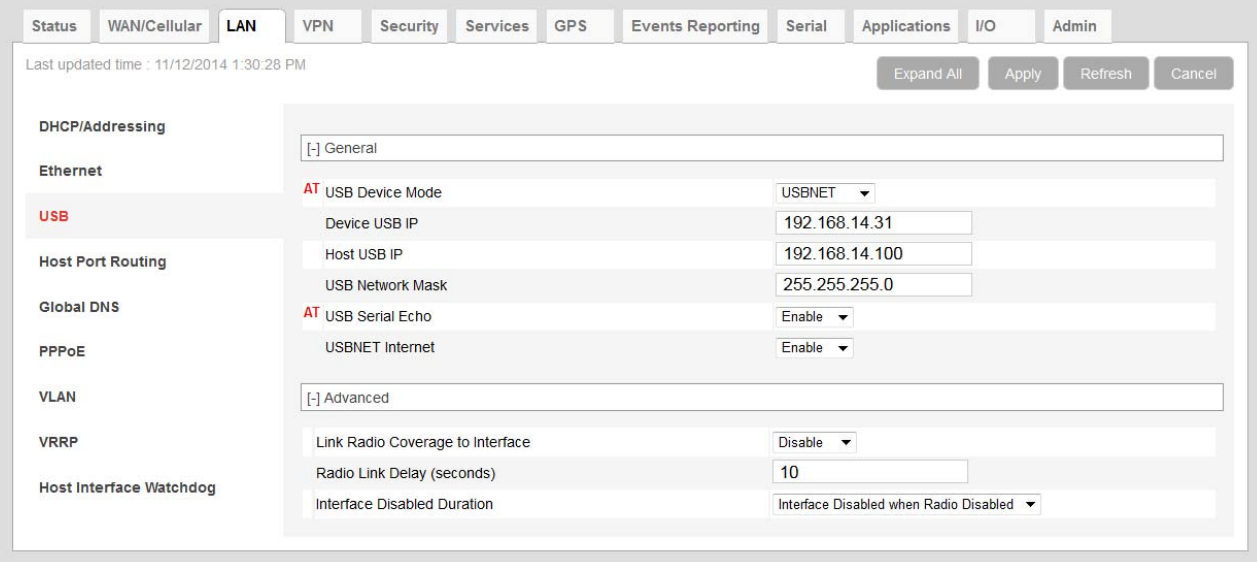


Figure 5-4: ACEmanager: LAN > USB

Field	Description
General	
USB Device Mode	*USBDEVICE=n • 0 — USB Serial • 1 — USBNET • 2 — Disabled This parameter alters the default startup data mode for the USB port. *Note: A reboot is required to activate the USB mode change.* *Note: If you want to stream GPS data to the USB port (Local/Streaming on page 247), set this field to USB Serial.*
Device USB IP	The USB/net IP address of the AirLink device. By default this is set to 192.168.14.31.
Host USB IP	The IP for the computer or device connected to the USB port

Field	Description
USB Network Mask	Use this field to configure a subnet mask for USBNET Default is 255.255.255.0
USB Serial Echo	Toggles AT command echo mode when the USB is configured for virtual serial 0 = OFF; 1 = ON
USBNET Internet	Enabled (default) or Disabled
Advanced	
Link Radio Coverage to Interface	Disables the specified port when there is no cellular coverage. Options are: • Disable (default) • Ethernet • USB
Radio Link Delay (seconds)	The delay in seconds before the selected interface goes down when there is no cellular coverage
Interface Disabled Duration	Sets the period of time (in seconds) that the LAN interface is disabled when linking a LAN port to radio coverage. Either the Ethernet or the USB LAN port can be linked to the radio coverage, but not at the same time. Options are: • Interface Disabled when Radio is disconnected (default) • 5 Sec • 10 Sec • 15 Sec • 20 Sec • 25 Sec • 30 Sec

Installing the USB Drivers

Note: You can download USBserial drivers for Windows XP, Windows 7, and Windows 8 from www.sierrawireless.com/Support/Downloads.aspx.

USBnet drivers are available for Windows XP 32-bit with SP3. (For information on SSP3, see http://support.microsoft.com/kb/322389). Windows XP with SP2 or earlier is no longer supported. For Windows 7 and Windows 8, you do not need to install a USBnet driver, as default Microsoft drivers are used.

USBserial and USBnet also work with Linux CDC-ACM drivers.

Virtual Ethernet is the default setting for the USB port. If you want to install the virtual serial port, change the Device Mode to USB Serial.

When you connect the AirLink device to a USB port on your computer for the first time, Windows detects a new device and prompts you to install the driver.

Note: Windows sees each port type as a different USB device and sees every port on your computer separately. If you change the port type on the AirLink device or connect to a different USB port on your computer or hub, Windows sees it as a new device.

The following instructions are for Windows XP:

1. To start the install of the USB virtual Ethernet driver, select No, not this time and click Next.

Found New Hardware Wizard
Welcome to the Found New Hardware Wizard
Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission).
Read our privacy policy
Can Windows connect to Windows Update to search for software?
Yes, this time only
Yes, now and every time I connect a device
No, not this time
Click Next to continue.
< Back
Next >
Cancel

Figure 5-5: Found New Hardware Wizard

2. Select Install from a list of specific location and click Next.

If your hardware came with an installation CD or floppy disk, insert it now.
What do you want the wizard to do?
Install the software automatically (Recommended)
Install from a list or specific location (Advanced)

Figure 5-6: Hardware Wizard: Location options

3. Select and/or enter the location of the driver.
   - If the driver is on the CD and the CD is in your drive, you can just select Search removable media.
   - If you have installed ACEmanager or the Setup Wizard, the drivers have been conveniently copied to your hard drive. Enter C:\Program Files\Common Files\AirLink as the location to search.
   - If you are installing the driver from a file downloaded from the Sierra Wireless website, select Include this location in the search and type in the location where you downloaded the file.
4. Click Next.

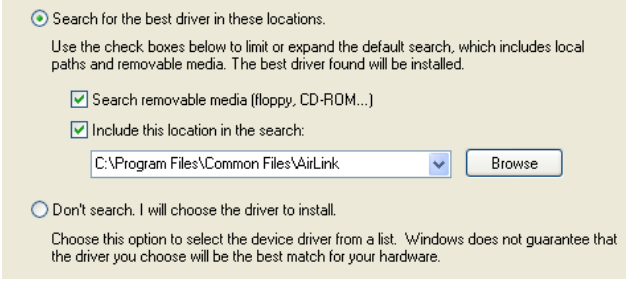

Search for the best driver in these locations.
Use the check boxes below to limit or expand the default search, which includes local paths and removable media. The best driver found will be installed.
Search removable media (floppy, CD-ROM...)
Include this location in the search:
C:\Program Files\Common Files\AirLink
Browse
Don't search. I will choose the driver to install.
Choose this option to select the device driver from a list. Windows does not guarantee that the driver you choose will be the best match for your hardware.

Figure 5-7: Hardware Wizard: Install location

After you select the location, the installation should begin. If you get a message asking if you want to continue the installation, click Continue Anyway.

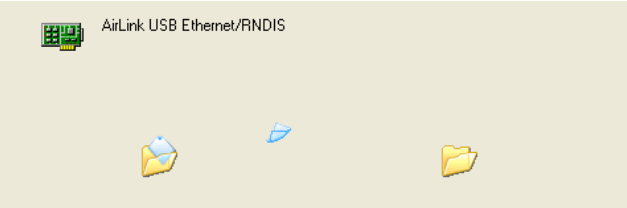


Figure 5-8: Hardware Wizard: Installing

5. Click Finish to complete the installation. The driver should be enabled without any need to reboot your computer.

Completing the Found New Hardware Wizard
The wizard has finished installing the software for:
AirLink USB Ethernet/RNDIS

Figure 5-9: Hardware Wizard: Finish

Virtual Ethernet

The USB Ethernet connection appears in your Network Connections page as a Local Area Connection.

Tip: *If you also have an Ethernet card on the computer, or have installed the USB Ethernet to more than one USB port on your computer, the USB Ethernet may show up with a number.*

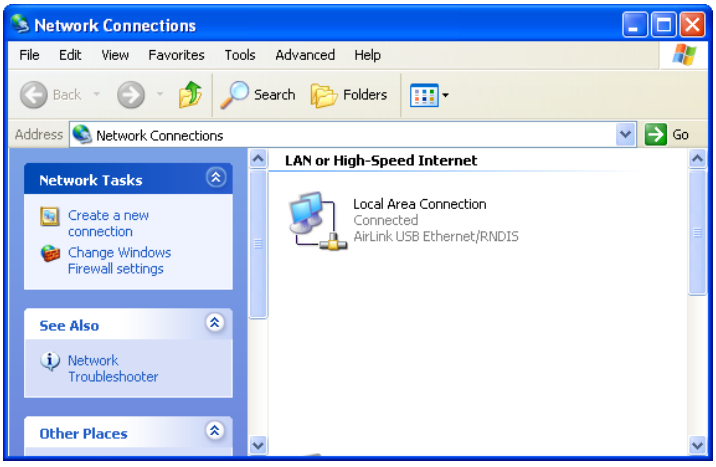


Figure 5-10: Network Connections

Note: By default, your Host IP for USB/net is 192.168.14.100.

You can also verify the installation by looking in the Device Manager.

1. Click Start > Control Panel.
2. Double-click the System icon.
3. Select the Hardware tab, and click the Device Manager button.

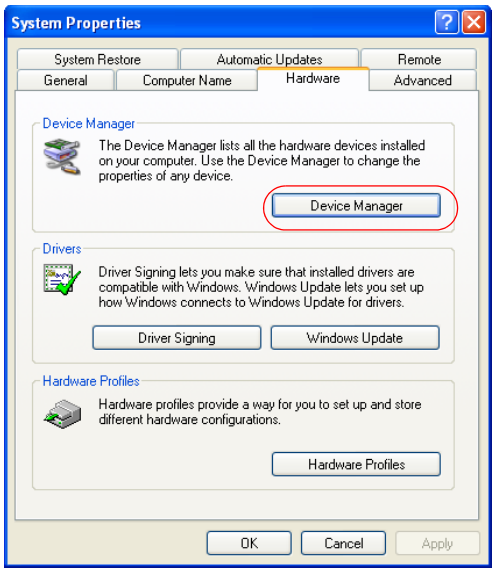

System Properties
System Restore
Automatic Updates
Remote
General
Computer Name
Hardware
Advanced
Device Manager
The Device Manager lists all the hardware devices installed on your computer. Use the Device Manager to change the properties of any device.
Device Manager
Drivers
Driver Signing lets you make sure that installed drivers are compatible with Windows. Windows Update lets you set up how Windows connects to Windows Update for drivers.
Driver Signing
Windows Update
Hardware Profiles
Hardware profiles provide a way for you to set up and store different hardware configurations.
Hardware Profiles
OK
Cancel
Apply

Figure 5-11: System Properties

4. Click the + in front of *Network Adapters*.

The newly installed driver, AirLink USB Ethernet/RNDIS, should appear.[1] If the driver is shown with a # and number behind the driver name (e.g., AirLink USB Ethernet/RNDIS #2), more than one is installed on your computer, most likely for a different USB port. More than one copy of the driver should not cause any problems since only the connected port and its driver would be active.

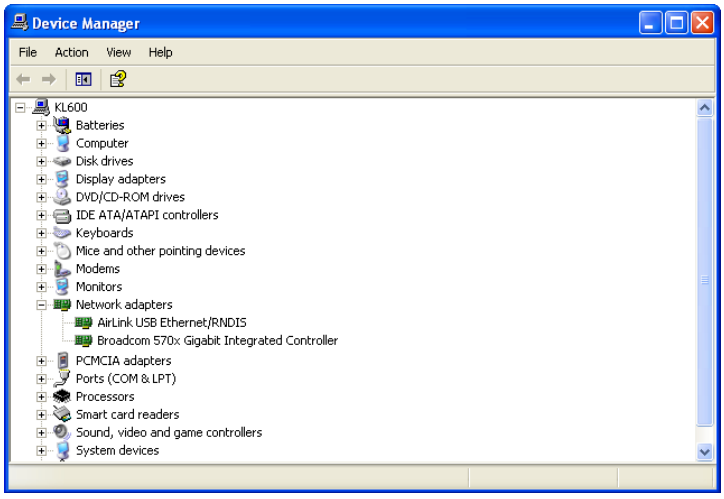


Figure 5-12: Device Manager > Ethernet

1. For Windows 7 and Windows 8, the driver should appear as “Remote NDIS based Internet Sharing Device”.

Once the driver is installed, you can use the USB port just like a standard Ethernet port.

Virtual Serial

Verify the installation by looking in the Device Manager.

1. Click Start > Control Panel.
2. Double-click the System icon.
3. Select the Hardware tab, and click the Device Manager button.

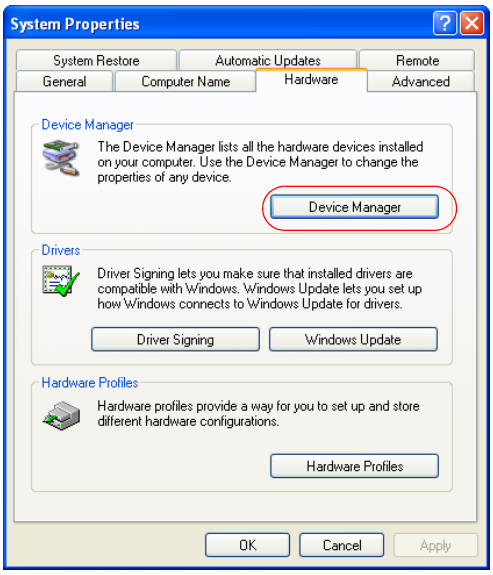

System Properties
System Restore
Automatic Updates
Remote
General
Computer Name
Hardware
Advanced
Device Manager
The Device Manager lists all the hardware devices installed on your computer. Use the Device Manager to change the properties of any device.
Device Manager
Drivers
Driver Signing lets you make sure that installed drivers are compatible with Windows. Windows Update lets you set up how Windows connects to Windows Update for drivers.
Driver Signing
Windows Update
Hardware Profiles
Hardware profiles provide a way for you to set up and store different hardware configurations.
Hardware Profiles
OK
Cancel
Apply

Figure 5-13: System Properties

4. Click the + in front of *devices*.

The newly installed driver, AirLink USB Serial Port, should appear.

Tip: *If the driver is shown with a number sign (#) and number behind the driver name (e.g., AirLink USB Serial Port #2), more than one driver is installed on your computer, most likely for a different USB port. More than one copy of the driver should not cause any problems since only the connected port and its driver would be active.*

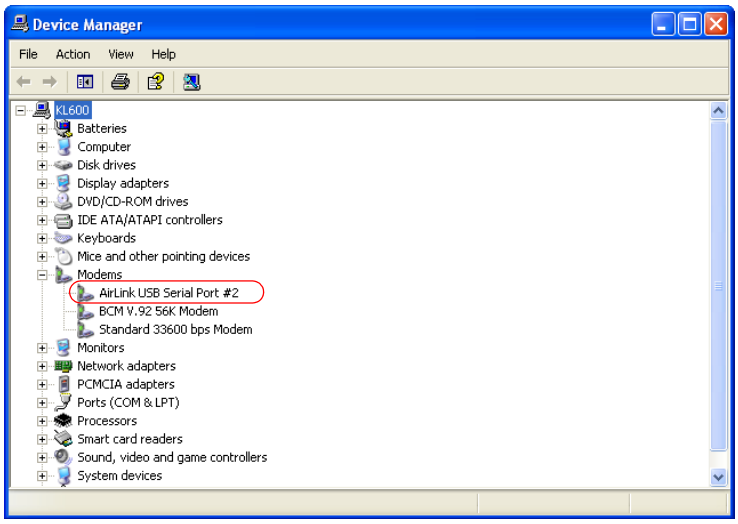


Figure 5-14: Device Manager > Serial

To connect to the device using the USB virtual serial, most applications or utilities require you to select or enter the serial (COM) port number. The USB connection appears as a standard serial port, so you need to determine its number to connect to it. The driver installation automatically assigns a port, or you can change it if you wish to another unused port.

5. From the Device Manager, right-click the driver name and select Properties.

Figure 5-15: Device Manager: Driver menu

6. Select the Advanced tab and click the Advanced Port Settings button.

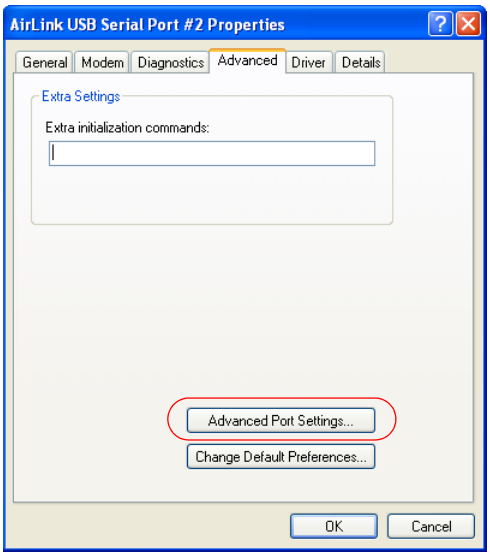


Figure 5-16: Driver Properties

7. The current port used is shown at the bottom of the screen. Use the drop-down menu to select an available COM port number if you need to change it.

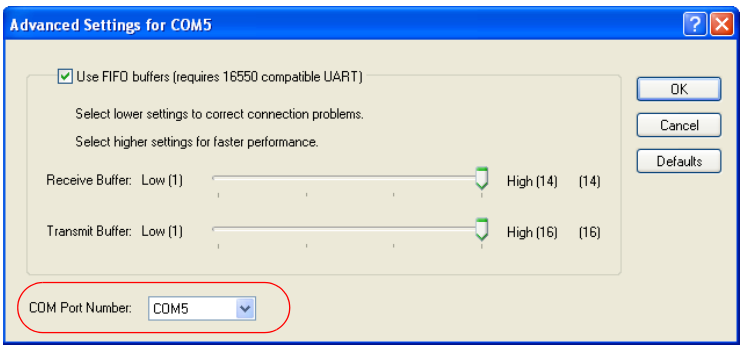


Figure 5-17: Advanced Settings

Note: The COM port number assigned by driver installation is the next port that is available.The port number might vary depending on the number of devices connected (using serial or virtual serial).

Once the driver is installed, you can use the USB port just like a standard serial port.

Host Port Routing

The Host Network is the equivalent of the IP route command.

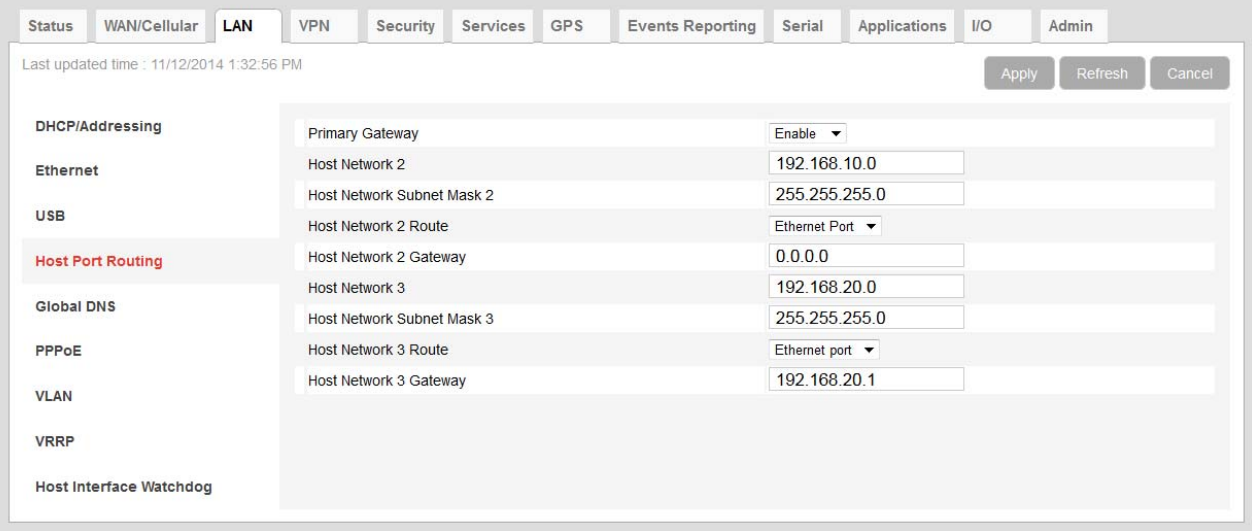


Figure 5-18: ACEmanager: LAN > Host Port Routing

Field	Description
Primary Gateway	When enabled, your AirLink device is the Primary Gateway for connected networks.
Host Network 2 and Host Network 3	Network to route to host interface connected to Ethernet Host Network 2 and 3 are secondary networks connected to the AirLink device. For example, 192.168.10.0.
Host Network Subnet Mask 2 and Host Network Subnet Mask 3	The subnet for the applicable network. For example, 255.255.255.0, which would with the setting above define a secondary network of 192.168.10.0/24.
Host Network 2 Route and Host Network 3 Route	Indicates what type of router is being used for the host network. If it is a traditional router which handles ARP for addresses on its subnet, select Ethernet. If it is a “dumb” gateway which is a conduit to a subnet but does not handle any ARP, select Gateway. When Gateway is selected, ALEOS will ARP for the destination address and send it to the defined Host Network Gateway address.
Host Network 2 Gateway and Host Network 3 Gateway	The IP address of the “dumb” Gateway. This should be left as 0.0.0.0 if the Host Network Route is Ethernet. Many routers respond to ARP requests for subnets behind the router. The default is Ethernet, which means that you do not have to configure the gateway IP. For those routers that do not respond to ARP requests for subnets, you need to enter the gateway address.

Wi-Fi

ALEOS provides Wi-Fi configuration capabilities and support for GX Series devices with a Wi-Fi X-Card installed.

The Wi-Fi X-Card works in one of three modes:

- Access Point (AP)
- Client (Wi-Fi WAN)
- Both (AP + Client)

The configuration options vary, depending on the mode selected.

Note: Wi-Fi fields appear ONLY if the Wi-Fi X-Card is installed in the AirLink GX Series device.

To configure the Wi-Fi settings:

1. In ACEmanager, go to LAN/Wi-Fi > Wi-Fi.

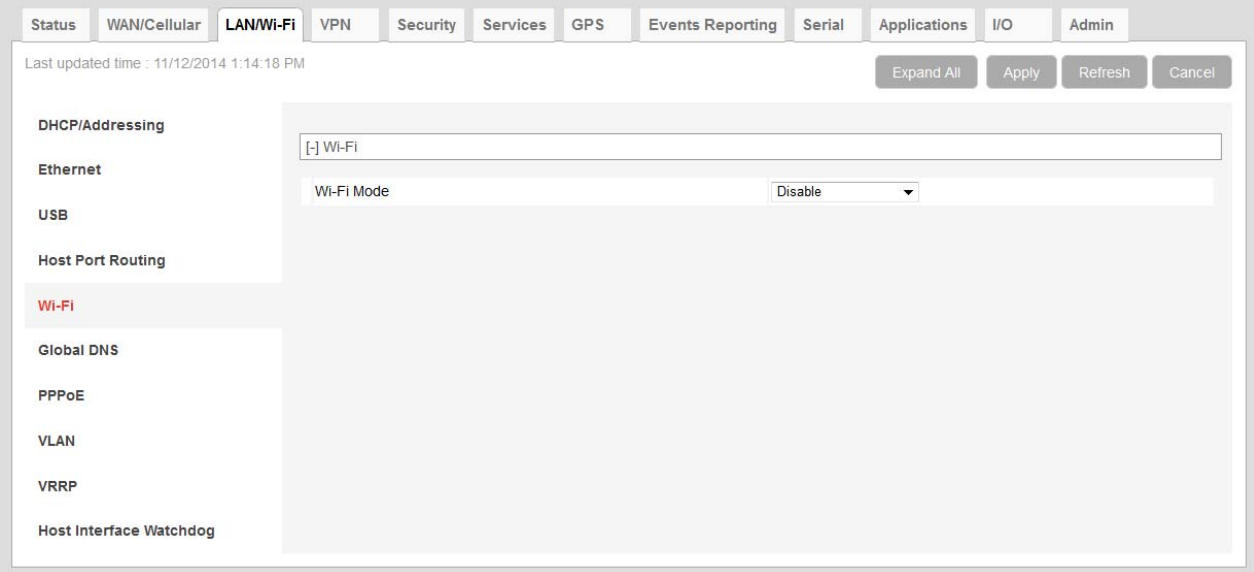


Figure 5-19: ACEmanager: LAN/Wi-Fi > Wi-Fi

Field	Description
Wi-Fi Mode	
Wi-Fi Mode	Allows you to choose the Wi-Fi mode of operation. Options are: • Disable (default) • Access Point (See page 130.) • Client (Wi-Fi WAN) (See page 134.) • Both (AP + Client) (See page 138.)

Access Point Mode

In this mode, the AirLink device acts as an access point.

To configure Access Point mode:

1. Select Access Point from the drop-down box in the Wi-Fi Mode field.
2. Click “+” beside Access Point to expand that section.

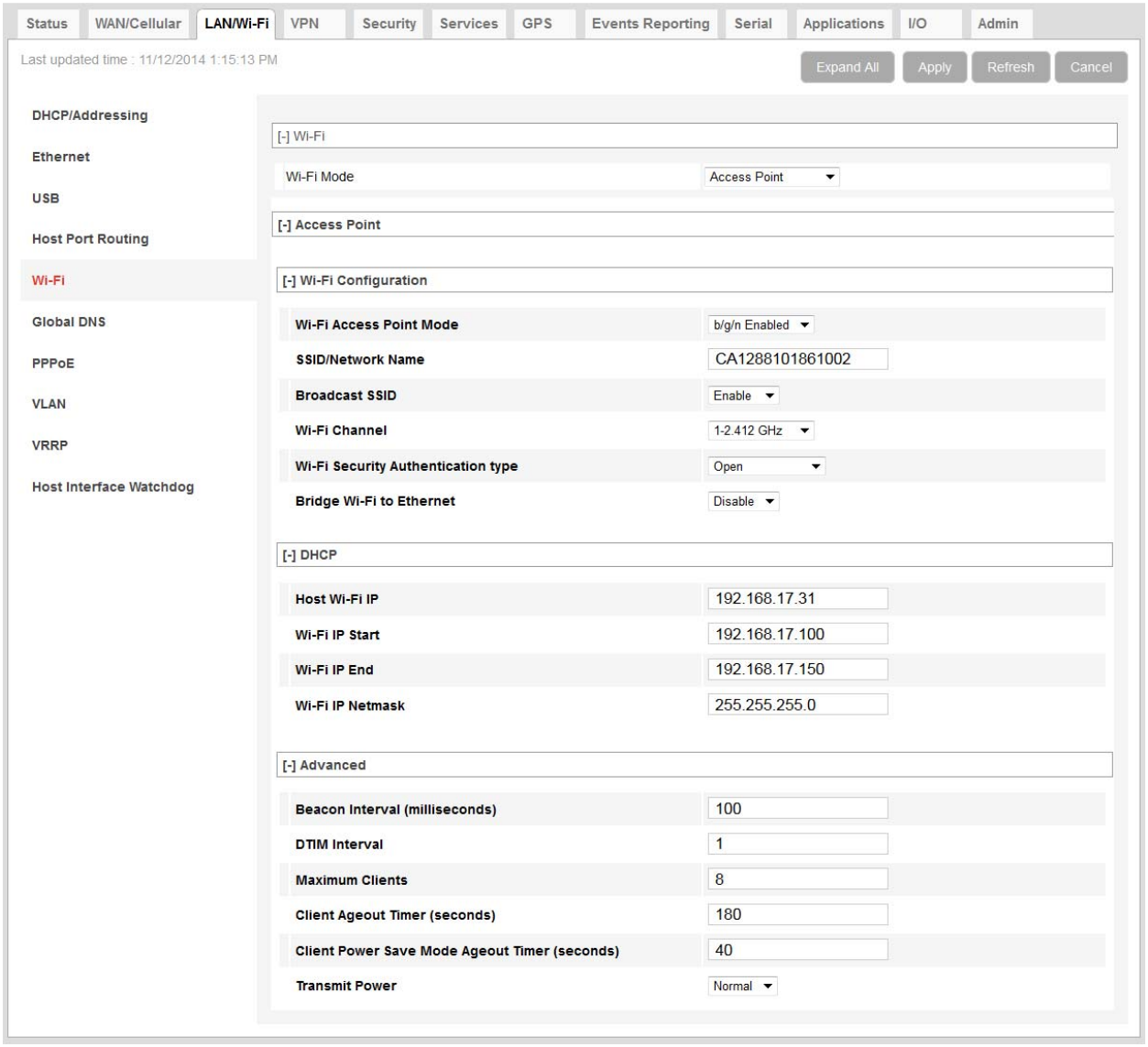


Figure 5-20: ACEmanager: LAN/Wi-Fi > Wi-Fi > Access Point

Field	Description
Wi-Fi Mode	
Wi-Fi Mode	See Wi-Fi Mode on page 115.

Field	Description
Wi-Fi Configuration	
Wireless Access Point Mode	The wireless access point mode configures operation for either 802.11b/g or b/g/n. Options are: • b/g Enabled • b/g/n Enabled (default) *Note: Selecting b/g/n Enabled limits the encryption options to Open and WPA/WPA2.*
SSID/Network Name	You can set the SSID/Network Name or it can be automatically generated (default). The SSID (Service Set Identifier) default value is the same as the AirLink GX Series device serial number which appears on the label on the bottom of the device. You can only configure one SSID. *Note: The SSID is case-sensitive.*
Broadcast SSID	Choose whether or not to broadcast the SSID Options are: • Enable (default)—SSID is broadcast • Disable—SSID is hidden (not broadcast) *Note: The option to hide the SSID is provided as a convenience and does not enhance security.*
Wi-Fi Channel	Select from 14 Wi-Fi channels. Options begin with Channel 1 at 2.412 GHz, and each subsequent channel increases in frequency by .005 GHz (*except* for Channel 14 which is at 2.484 GHz). Default: 1–2.412 GHz. *Note: Some channels are not available for specific geographical areas.*
Wi-Fi Security Authentication type	Select the authentication type. Options are: • Open—No authentication is needed when this option is selected. This option allows any user to connect to the AP and is generally not recommended. When you select Open (and bg Enabled in the Wi-Fi Access Mode field) WEP authentication options are available. See Open WEP on page 133. • WPA Personal • WPA2 Personal
Bridge Wi-Fi to Ethernet	This field allows you to create a unified bridge between the AirLink's device's Wi-Fi and Ethernet interfaces. Options are: • Enable—Ethernet and Wi-Fi are on the same subnet. The Wi-Fi hosts get their DHCP IP addresses from the Ethernet pool (when Ethernet DHCP is enabled). This also allows interface routing between the Ethernet and Wi-Fi hosts. (default) • Disable—Wi-Fi is a separate LAN subnet from the Ethernet LAN. There is no routing between the two interfaces and their connected hosts.
DHCP Available only when the Wi-Fi has its own subnet (Bridge Wi-Fi to Ethernet is disabled.)	
Host Wi-Fi IP	Displays the AP's IP address. Default: 192.168.17.31

Field	Description
Wi-Fi IP Start	Displays the beginning IP address to be served. Default: 192.168.17.100
Wi-Fi IP End	Displays the ending IP address to be served. Default: 192.168.17.150
Wi-Fi IP Netmask	Displays the subnet IP netmask of the Wi-Fi network. Default: 255.255.255.0
Advanced	
Beacon Interval (milliseconds)	How frequently the AirLink device sends periodic message (beacons) to advertise its availability (in milliseconds) Options are: • 1–65535 milliseconds (Default is 100)
DTIM Interval	The number of beacons the client device can sleep through before waking up to check for messages For example, if the DTIM Interval is set to 3, the client wakes up every third beacon. The higher the setting in the DTIM Interval field, the longer the client device can sleep, and the more battery power the client device can potentially save. However, high DTIM intervals can also reduce throughput to the client. Options are: • 1–255 (Default is 1.)
Maximum Clients	Indicates the maximum number of concurrent users (clients) supported Options: • 1 to 8 (Default is 8.)
Client Ageout Timer (seconds)	The length of time a client (not in power save mode) is inactive (does not transmit any traffic) before the Access Point detaches the client Options are: • 0–3600 seconds (Default is 180.)
Client Power Save Mode Ageout Timer (seconds)	The length of time a client (in power save mode) is inactive (does not transmit any traffic) before the Access Point detaches the client Options are: • 0–3600 seconds (Default is 180.)
Transmit Power	Adjusts the transmit power of the AP. Options are: • Normal —16 dB (default) • Low—10 dB *Note: For information on the Wi-Fi range, refer to the GX Series Hardware User Guide.*

When you choose the b/g Enabled option in the Wi-Fi Access Point Mode field, and Open in the Wi-Fi Security Authentication type field, an additional section for Open WEP appears:

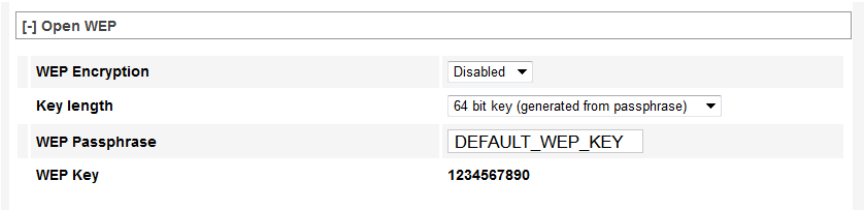


Figure 5-21: ACEmanager: LAN/Wi-Fi > Access Point Open WEP section

Field	Description
Open WEP	
Note: WEP is not a recommended Wi-Fi Security protocol because of its well publicized vulnerabilities. Use WPA/WPA2 Personal instead. Only alphanumeric characters can be used for the WEP passphrase. WEP is only available if the Enable Wireless Access Point field is set to b/g Enabled. (See Wireless Access Point Mode on page 131.)	
WEP Encryption	Enable or disable WEP encryption Options are: • WEP —WEP encryption • Disabled (default)
Key length	Length of the security key to use Options are: • 64 bit key (generated from passphrase) (default) • 128 bit key (generated from passphrase) • Custom Key—64 or 128 bit key (user specifies 5 or 10 hex characters)
WEP Passphrase	WEP passphrase to be used • 10–255 alphanumeric ASCII characters This field does not appear if the Custom Key option is selected in the Key length field.
WEP Key	Displays the WEP key in hex characters The WEP Key is generated from the WEP Passphrase when you select 64-bit key or 128-bit key in the Key length field*. This is the Key required by AP clients to connect to the device. To generate the WEP Key: 1. Set the Key length. 2. Enter the WEP Passphrase. 3. Click Apply. 4. Reboot the device. The current WEP Key is displayed in ACEmanager only after rebooting. * If you selected Custom Key in the Key length field, enter the desired custom key in hex characters only (5–10 hex characters). When logging in with a Custom Key, you can enter the hex characters or the ASCII equivalent. For example, if the custom key is 68656c6c6f, you can log in using 68656c6c6f or the ASCII equivalent (hello).

If WPA Personal or WPA2 Personal are selected for the Wi-Fi Security Authentication type field, a WPA/WPA2 Personal section replaces the Open WEP section in the user interface.

Figure 5-22: WPA/WPA2 security options

Field	Description
WPA/WPA2 Personal	
Wi-Fi Encryption	Specify the encryption type for WPA or WPA2 authentication. Options are: • TKIP—Available for 802.11b/g, not available for 802.11n. • AES (default) *Note: If WPA2 is selected as the authentication type (see Wi-Fi Security Authentication type on page 131) only AES is available.*
WPA Passphrase	Specify the WPA Passphrase AP clients use to connect to the device. Minimum length is 8 characters and maximum length is 64. Default: None.

Client (Wi-Fi WAN) Mode

In Client Mode, the AirLink GX Series device acts as a Wi-Fi client and can connect to an access point. While connected, the Wi-Fi link is primarily an uplink for the AirLink device and all connected hosts. All outbound traffic is routed over the Wi-Fi connection instead of the mobile broadband connection.

Client Mode has been tested with the top 5 WLAN Access Point vendors: Cisco®, Aruba Networks®, Motorola™, HP®, and NETGEAR®.

You can configure up to 10 Access Points for each AirLink GX Series device. Only one Access Point is used at a time for the client connection. Having additional APs configured allows for portability. Since the AirLink device generally runs unattended, it does not do a broadcast discovery to display all available APs in the area. You need to know the specific configuration details for the APs you want to configure in ACEmanager.

Note: When the GX device is in Wi-Fi client mode, it uses the DHCP router option value to determine the default gateway. If the DHCP server or DHCP relay agent has more than one router in the router option list, the GX device uses the first router in the list as the default gateway.

Select Client Mode in the Wi-Fi Mode field, and click “+” beside Client Mode to expand that section.

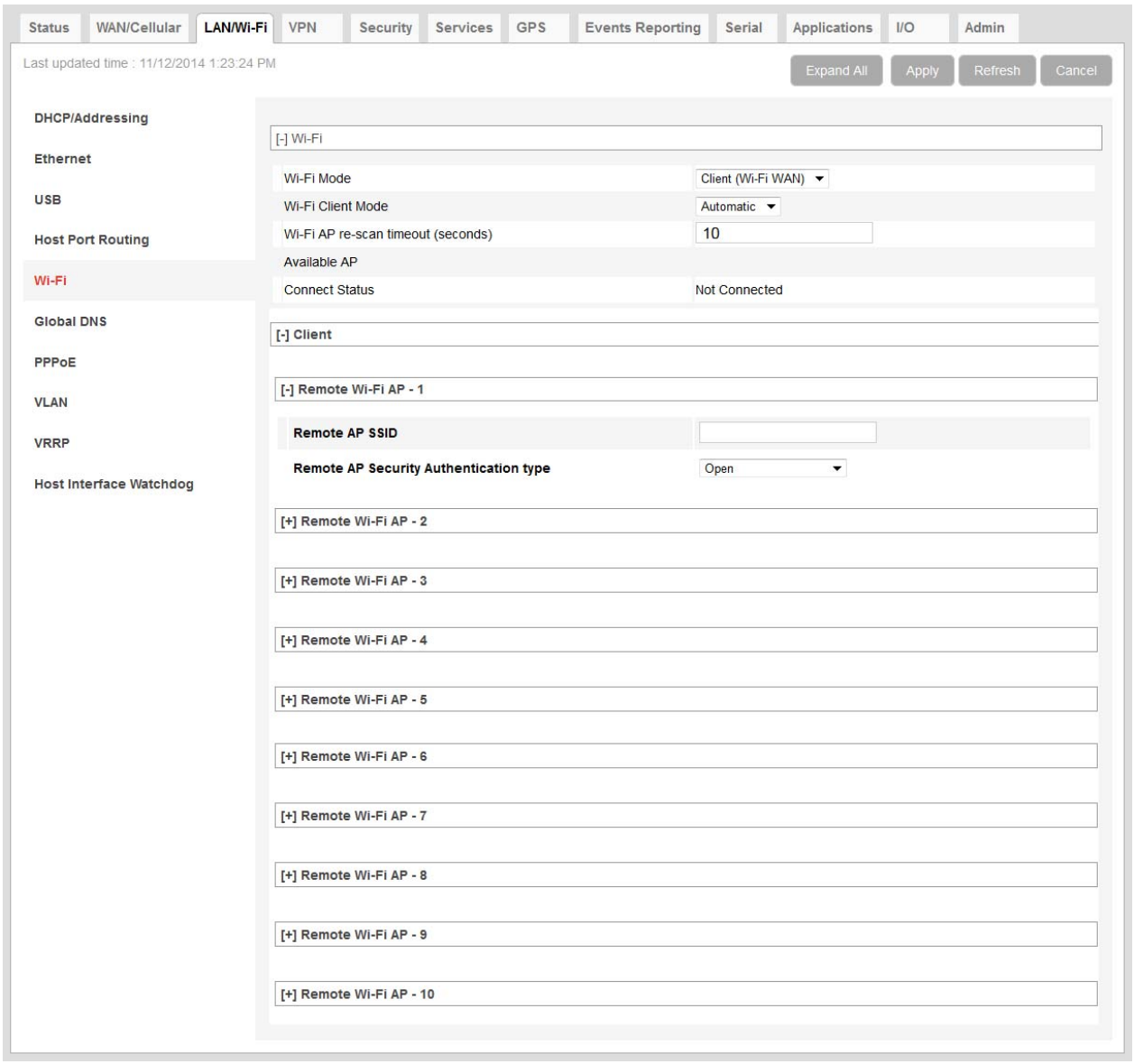


Figure 5-23: ACEmanager: LAN/Wi-Fi > Wi-Fi > Client Mode > Automatic

Field	Description
Wi-Fi Mode	
Wi-Fi Client Mode	Allows you to choose the connection mode. Options are: • Automatic (default)—The WAN connection automatically switches from the mobile broadband network to Wi-Fi whenever a configured Wi-Fi Access Point (AP) is within range. When automatic is selected, the AirLink device scans for the first AP on the configured list. If the first AP is not available (i.e. signal strength is less than -90 dBm), it scans for the next one on the list. It continues scanning the configured APs until it finds an available one. When it finds an available AP, the AirLink device switches from the mobile broadband network to the AP's Wi-Fi network. If the AirLink device gets to the end of the list without finding an available AP, it begins again at the top of the list. The AirLink device tries to connect to each configured AP for 3 seconds. If it fails to connect to any of the APs in the list, before beginning again at the top of the list, it waits for the Wi-Fi rescan timeout period. For more information about using Automatic Wi-Fi Client Mode, refer to the AirLink GX Series Hardware User Guide. Field description continued on page 137.

Field	Description
Wi-Fi Client Mode (continued)	• Manual When Manual is selected, click the Connect button to connect to an available access point. You can also use ACEview to manually connect to the access point: 1. Open ACEview and go to Menu > View > Wi-Fi. 2. ACEview displays a list of available access points and the connection state. 3. Select an available AP, and click Connect. A message window appears asking if you want to connect the available Access Point. 4. Click OK. *Note: Whenever configuring or changing the Wi-Fi Client Mode from Automatic to Manual or Manual to Automatic, you must reboot the device. The device begins checking for available APs once the reboot is complete.*
Wi-Fi AP rescan timeout (seconds)	This field only appears in Client (Wi-Fi WAN) mode when it is set to Automatic. Determines how often the AirLink device re-scans for a configured Access Point when it is not connected to an Access Point. Options are: • 10—3600 seconds (default is 10 seconds) *Note: When the device is in Client (Wi-Fi WAN mode) it is best to leave the default value.*
Available AP	Identifies the currently available access point Only one AP is shown, even if additional APs are configured and in range. If there is more than one AP available in the area, the first one in the list with signal strength greater than -90 dBm is displayed.

Field	Description
Connect	This button only appears when the Manual Wi-Fi Client Mode is selected. In manual mode, click the connect button to connect to an available access point.
Connect Status	Indicates whether or not the GX device is connected to an access point.
Remote Wi-Fi AP - 1, Remote Wi-Fi AP - 2... Remote Wi-Fi AP - 10	
Remote AP SSID	Use this field to configure the remote access point you want the AirLink GX device to be able to scan for and connect to. The GX device scans for available APs in the order they are configured in ACEmanager, so you may want to configure the most commonly used AP as Remote Wi-Fi AP 1. *Note: The SSID is case-sensitive. The configured parameters for the remote AP must be accurate. The AirLink device does not prompt if there is a mismatch.*
Remote AP Security Authentication type	Use this field to configure the authentication type used by the access point. Options are: • Open—No authentication is needed when this option is selected. Connecting to an Open (no authentication) AP is generally not recommended. (default) • WPA/WPA2 Personal • WEP—Connecting to a WEP AP is generally not recommended since it offers very low authentication/encryption. *Note: If the Access Point requires a secondary authentication through a landing page, the GX device cannot enter those credentials. This type of AP may not allow full functionality for the GX device.*
Remote AP WPA Passphrase	For APs using WPA or WPA2, enter the WPA Passphrase for the Wi-Fi Access Point.
WEP Key	For APs using WEP, enter the WEP Key for the Wi-Fi Access Point.

Both (AP + Client) Mode

In this mode, the AirLink GX device:

- Acts as an access point for other devices
- Connects to configured access points as a Wi-Fi client

For more information on using this mode, refer to the GX Series Device Hardware User Guide.

When you select this mode, you can configure the Access Point and Client fields in one page. (Click “+” beside each section to expand it.)

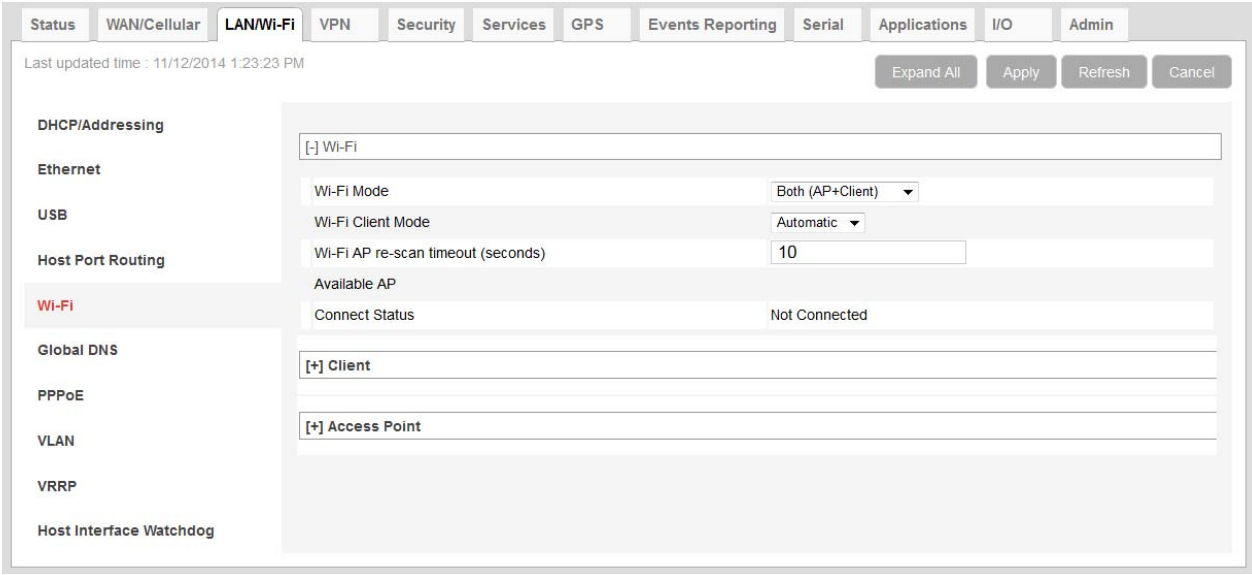


Figure 5-24: ACEmanager: LAN/Wi-Fi > Wi-Fi > Both (AP + Client) Mode

Wi-Fi Mode	
Wi-Fi AP rescan timeout (seconds)	Determines how often the AirLink device re-scans for a configured Access Point when it is not connected to an Access Point. Options are: • 10—3600 seconds (default is 10 seconds) *Note: For most use cases, it is best to leave the default value, but in some cases, the GX may drop the cellular connection to the Internet while scanning for an Access Point. If this is occurring, especially if there are no available Access Points, you can increase the timeout period to minimize the frequency of lost connections.*
For information on configuring all other fields, see Access Point Mode on page 130 and Client (Wi-Fi WAN) Mode on page 134.	

Note: If any of the configured APs that the GX device connects to have authentication configured, the authentication on the Access Points must be set to Open.

Global DNS

When the cellular network grants the IP address to the device, it includes the IP addresses of its DNS servers. Global DNS allows you to override the Mobile Network Operator's DNS settings for all connected devices. This is useful when the connected devices need to use a private network.

Note: If there are no alternate DNS servers defined, the default is the WAN network DNS server.

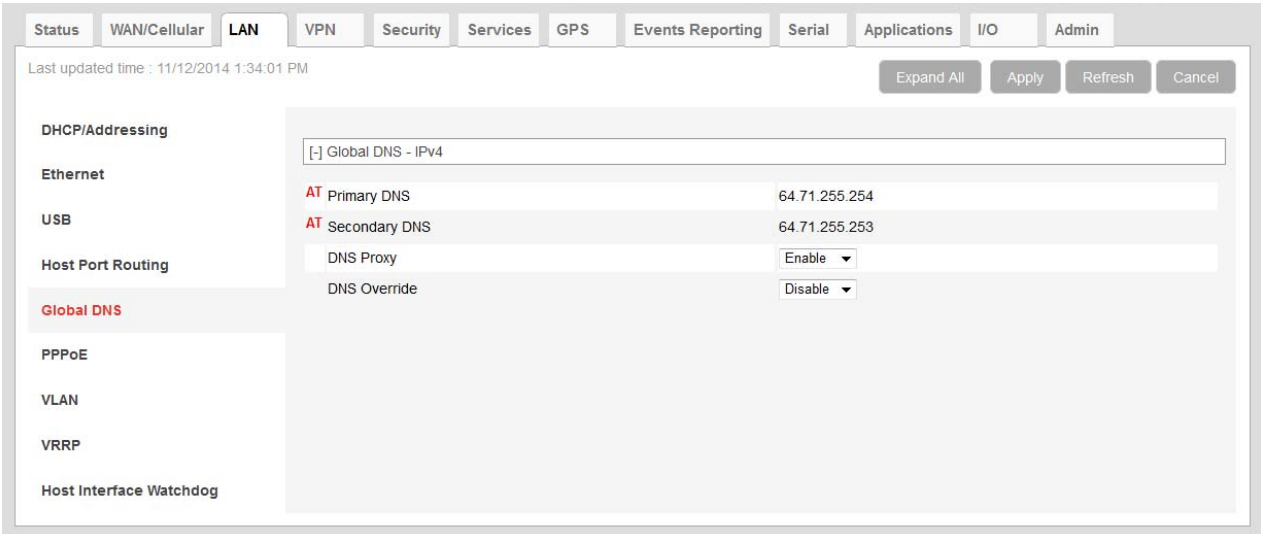


Figure 5-25: ACEmanager: LAN > Global DNS

Field	Description
Primary DNS	Primary Mobile Network Operator's DNS IP Address. This and the secondary DNS are generally granted by the cellular network along with the Network IP.
Secondary DNS	Secondary Mobile Network Operator's DNS IP Address

DNS Proxy	Determines whether or not the AirLink device is used as a DNS proxy server.
	Note: Using the AirLink device as a proxy DNS server can help reduce mobile network data use.
	Options are:
	• Enable (default) —All connected DHCP clients (PPP, PPPoE, Wi-Fi, USBNET, and Ethernet) send their DNS IP address resolution requests to the AirLink device. The AirLink device performs DNS lookups on behalf of the DHCP client.
	  • If the AirLink device is able to resolve the request, it sends a response to the DHCP client.
	  • If the AirLink device does not have the necessary information to resolve the request, it sends the request to the DNS server configured in the DNS Override field. When the AirLink device receives a response, it forwards it to the DHCP client and saves the information so that it can resolve the same request in the future.
	• Disable—All connected DHCP clients send their DNS IP address resolution requests to the DNS server received from the mobile network or the alternate server specified by DNS Override, if enabled. The AirLink device is not used as a DNS server.

DNS Override	Overrides the Mobile Network Operator's DNS address with the DNS server configured in the Alternate Primary DNS and Alternate Secondary DNS fields. Options are: • Disable (default)—Mobile Network Operator's DNS server is used • Enable—Alternate DNS server is used

Field	Description
Alternate Primary DNS	Configure the primary DNS server to use instead of the Mobile Network Operator's DNS server
Alternate Secondary DNS	Configure the secondary DNS server to use instead of the Mobile Network Operator's DNS server
Alternate DNS Port	If you want to specify the port on the connected device that the AirLink device sends IP address resolution responses to: 1. Ensure that the DNS Override field is set to Enable. 2. Enter the desired port number in this field. 3. Click Apply. When this field is set to 53 (default) or 0, packets are sent to port 53, the standard DNS port.

PPPOE

PPPoE (Point-to-Point Protocol over Ethernet) allows a point-to-point connection while using Ethernet. Just like the dial up protocol on which it is based, PPPoE can use traditional user name and password authentication to establish a direct connection between two Ethernet devices on a network (e.g., your AirLink device and your computer or router).

examples for PPPoE with your AirLink device:

- Backup connectivity solution for your network
- Individualized Internet connection on a LAN
- Password restricted Internet connection

Only one computer, router, or other network device at a time can connect to the AirLink device using PPPoE. If you are using the AirLink device connected to a router as a back up Internet connection for your network, you should configure the router to use the PPPoE connection and not the individual computers.

Note: To configure a PPPoE connection on some operating systems, you need administrator privileges to the computer you are configuring or access granted by an administrator on the network to add/remove devices to your computer.

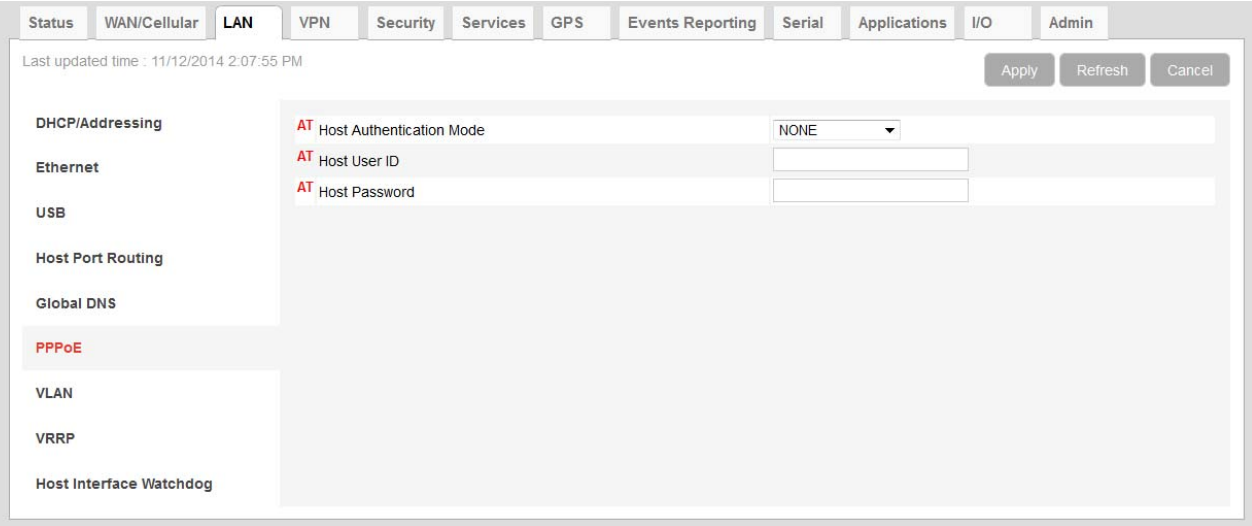


Figure 5-26: ACEmanager: LAN > PPPoE

Field	Description
Host Authentication Mode	Host Authentication Mode: Use PAP or CHAP to request the user login and password during PPP or CHAP negotiation on the host connection. The username and password set in *HOSTUID and *HOSTPW is used. • NONE (default) • PAP and CHAP • CHAP
Host User ID	User ID for authentication (up to 64 bytes)
Host Password	Password for authentication

Configure the AirLink Device to Support PPPoE

Note: You must disable the DHCP server for PPPoE to work.

To configure an AirLink device to support PPPoE:

1. In ACEmanager, go to LAN > Ethernet.
2. Under General, in the DHCP Server Mode field, select Disable.

Note: PPPoE authentication is optional. If you use PPPoE authentication, no other tethered LAN connection will have network access, regardless of whether or not the PPPoE host is connected. If you are using non-authenticated PPPoE, other tethered LAN connections will have network access until a PPPoE host is connected.

3. If you want to use authenticated PPPoE:

a. Go to LAN > PPPoE, and in the Host Authentication Mode field, select PAP and CHAP.

b. In the Host User ID, enter a user ID for the PPPoE connection.

c. In the Host Password field, enter a password for the PPPoE to connection.

4. Click Apply.
5. Reboot the device.

Tip: *If you leave Host User ID and Host Password blank, any computer or device can connect to the AirLink device using PPPoE.*

Note: ACEmanager shows the existing value for the PPPoE password as stars (****).

Optional: Configure the Device Name

1. In ACEmanager, go to Services > Dynamic DNS.
2. In the Service field, select IP Manager.
3. Under Dynamic IP, enter a name in the Device Name field, such as AirLink device or the ESN. The name can be up to 20 characters long.

   The name you choose for Device Name does not affect the connection, but may need to be configured in PPPoE settings for the router, device, or computer you connect to your AirLink device.

Configuring a PPPoE Connection in Windows 7

1. In Windows 7, go to Start > Control Panel.

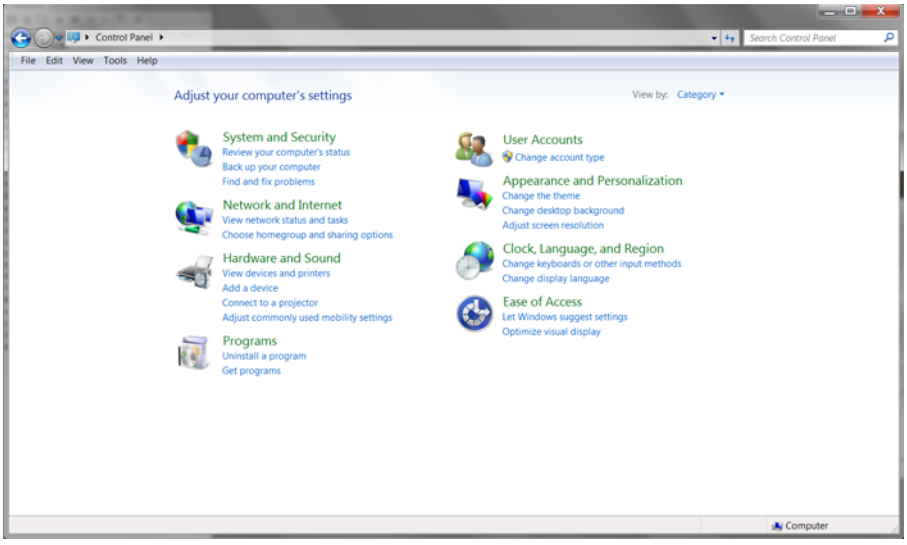


Figure 5-27: Windows 7: Control Panel

2. Select Network and Internet.

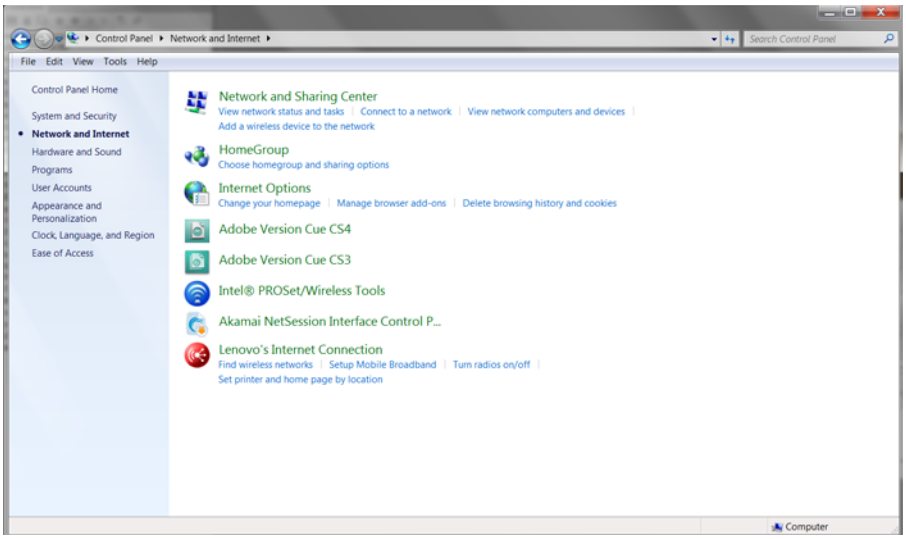

Control Panel ▸ Network and Internet ▸
Search Control Panel
File Edit View Tools Help
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock, Language, and Region
Ease of Access
Network and Sharing Center
View network status and tasks | Connect to a network | View network computers and devices
Add a wireless device to the network
HomeGroup
Choose homegroup and sharing options
Internet Options
Change your homepage | Manage browser add-ons | Delete browsing history and cookies
Adobe Version Cue CS4
Adobe Version Cue CS3
Intel® PROSet/Wireless Tools
Akamai NetSession Interface Control P...
Lenovo's Internet Connection
Find wireless networks | Setup Mobile Broadband | Turn radios on/off
Set printer and home page by location
Computer

Figure 5-28: Windows 7: Control Panel > Network and Internet

3. Select Network and Sharing Center.

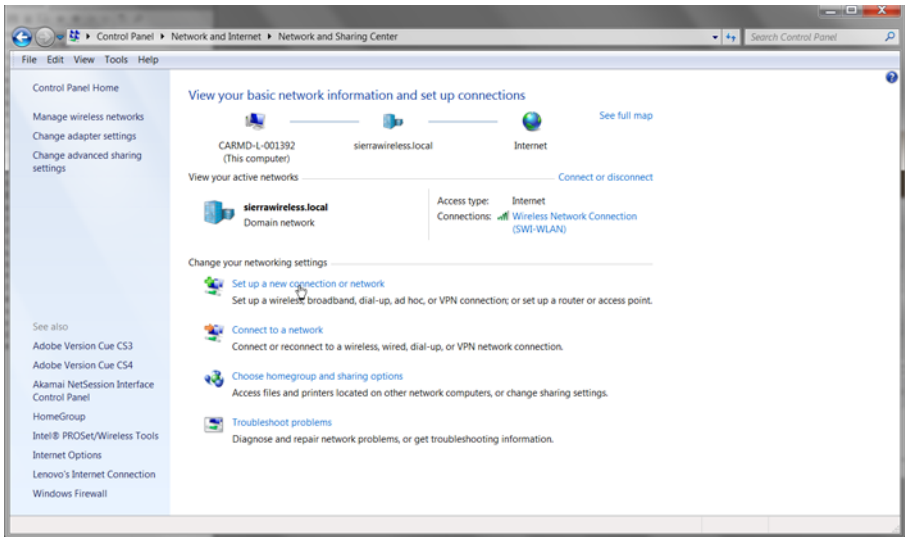

Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search Control Panel
File Edit View Tools Help
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
CARMD-L-001392 (This computer)
sierrawireless.local
Internet
View your active networks
Connect or disconnect
sierrawireless.local
Domain network
Access type: Internet
Connections: Wireless Network Connection (SWI-WLAN)
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.
Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
Adobe Version Cue CS3
Adobe Version Cue CS4
Akamai NetSession Interface Control Panel
HomeGroup
Intel® PROSet/Wireless Tools
Internet Options
Lenovo's Internet Connection
Windows Firewall

Figure 5-29: Windows 7: Control Panel > Network and Sharing Center

4. In the middle of the page, under Change your networking settlings, select Set up a new connection or network.

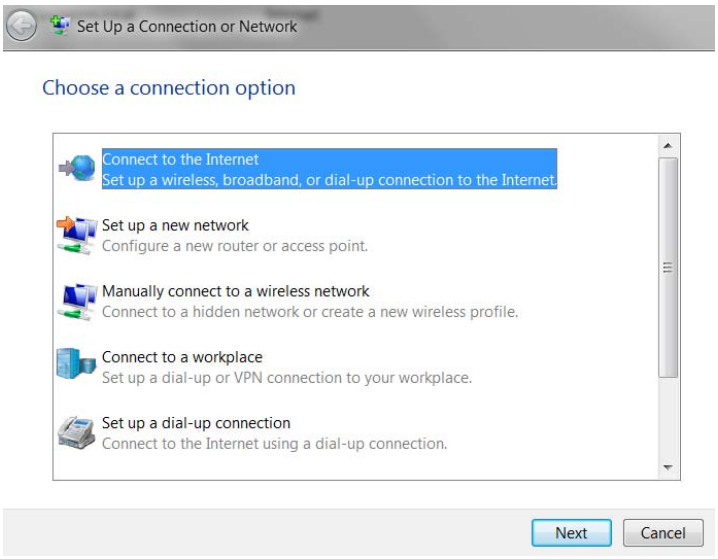
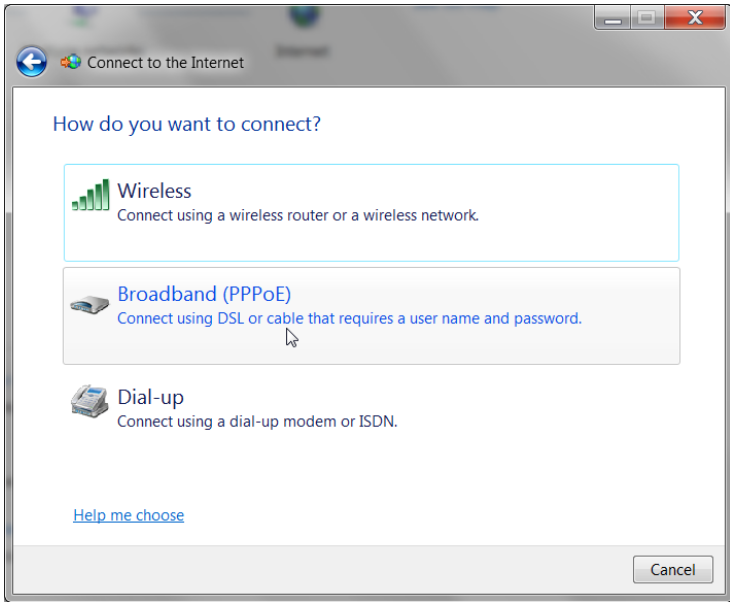
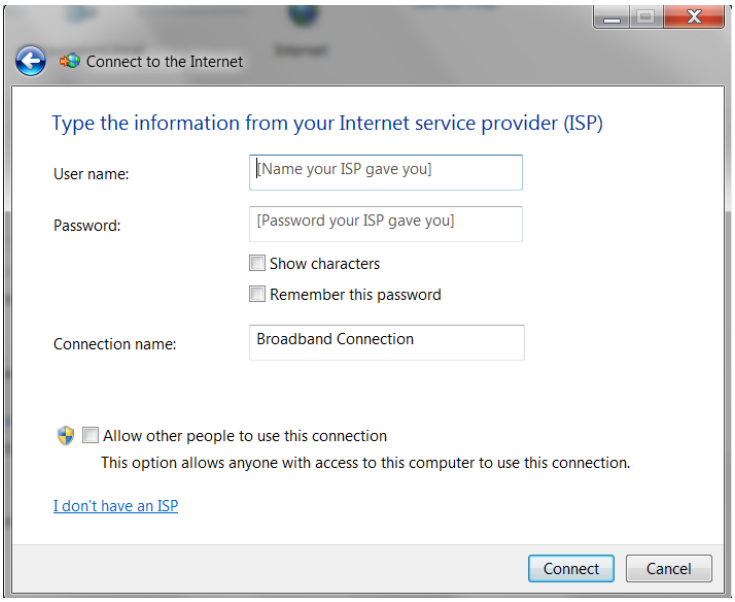

Set Up a Connection or Network
Choose a connection option
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.
Set up a new network
Configure a new router or access point.
Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.
Set up a dial-up connection
Connect to the Internet using a dial-up connection.
Next
Cancel

Figure 5-30: Set Up an Connection or Network

5. Select Connect to the Internet and click Next.


Connect to the Internet
How do you want to connect?
Wireless
Connect using a wireless router or a wireless network.
Broadband (PPPoE)
Connect using DSL or cable that requires a user name and password.
Dial-up
Connect using a dial-up modem or ISDN.
Help me choose
Cancel

6. Select Broadband (PPPoE).


Connect to the Internet
Type the information from your Internet service provider (ISP)
User name:
[Name your ISP gave you]
Password:
[Password your ISP gave you]
Show characters
Remember this password
Connection name:
Broadband Connection
Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.
I don't have an ISP
Connect
Cancel

7. If you are using authenticated PPPoE, enter the User name and Password you configured in ACEmanager.
8. If desired, change the Connection name to something such as PPPoE that clearly identifies the connection.
9. Click Connect.

For subsequent connections, you can click the network icon in the Task bar ( ) and select the PPPoE connection.

VLAN

ALEOS supports up to three Virtual Local Area Networks (VLANs) on its Ethernet port. VLANs are logical groupings of network devices that share the same broadcast domain. All devices on the same VLAN can ping each other without routing. ALEOS does not support routing between VLANs.

Note: The VLANs must also be configured on the switch.

Figure 5-31 shows a network configured for two VLANs.

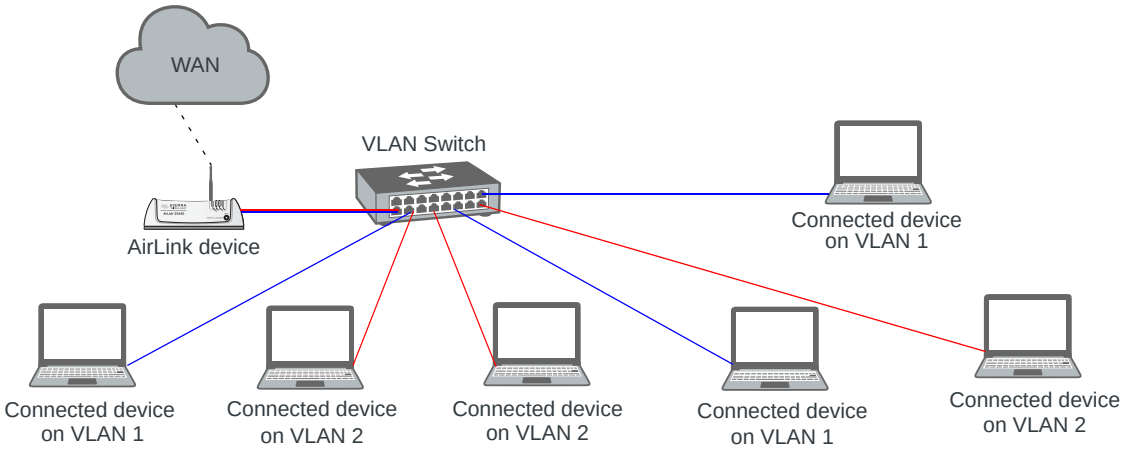


Figure 5-31: VLAN network configuration

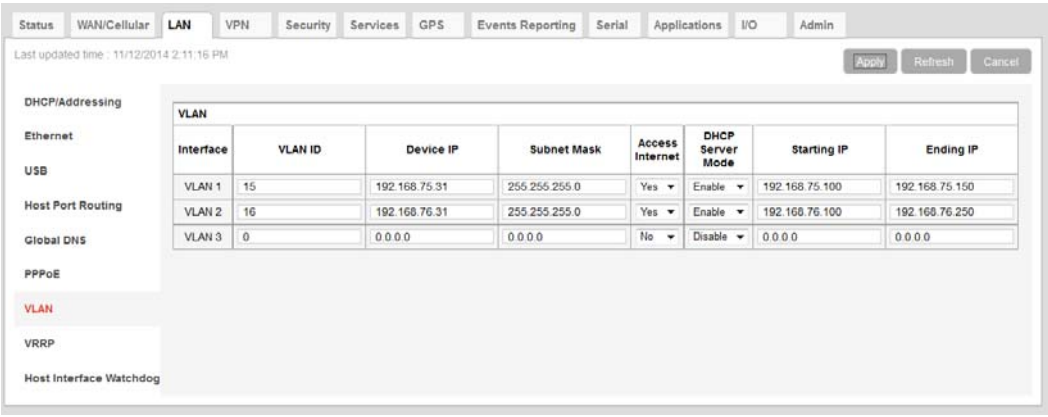


Figure 5-32: ACEmanager: LAN > VLAN

Field	Description
Interface	Displays the three VLANs you can configure
VLAN ID	VLAN ID • 0—VLAN is disabled (default) • 1–4094—Valid range for VLAN ID
Device IP	The IP address of the AirLink device for that VLAN interface
Subnet Mask	The subnet mask indicates the range of host IP addresses that can be reached directly. Changing the subnet mask limits or expands the number of devices that can connect to the AirLink device.
Access Internet	Choose whether or not devices on the configured VLAN have access to the Internet. • Yes • No

Field	Description
DHCP Server Mode	Choose whether or not the AirLink device acts as a DHCP server Options are: • Enable—AirLink device acts as the DHCP server • Disable (default)
Starting IP	VLAN interface DHCP pool starting IP address
Ending IP	VLAN interface DHCP pool ending IP address

VRRP

VRRP (Virtual Router Redundancy Protocol) enables you to configure a backup WAN connection to be used if the primary connection fails. You can configure VRRP on the AirLink device's Ethernet port or for VLANs.

You configure a VRRP Master and VRRP Backup device(s) and set their priorities. The device with the highest priority (normally the VRRP Master) becomes the primary route for the data connection.

The VRRP Master and Backups share a common virtual IP.

For information on configuring VLANs, see VLAN on page 146.

One common scenario is to use a 3rd party router for the primary connection and the AirLink device, either with or without VLANs, for the backup connection, as shown in Figure 5-33 and Figure 5-34.

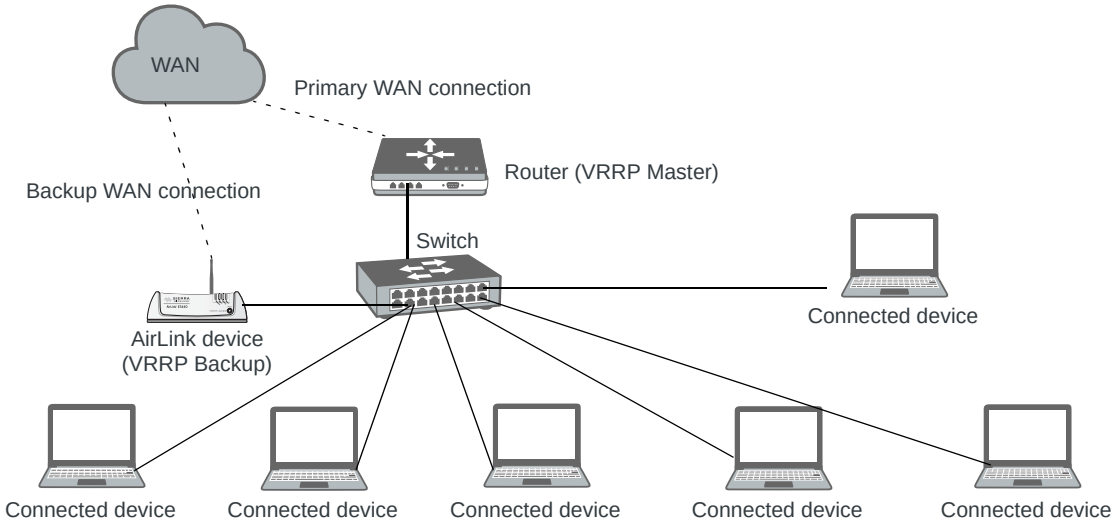


Figure 5-33: VRRP Network Configuration without VLANs

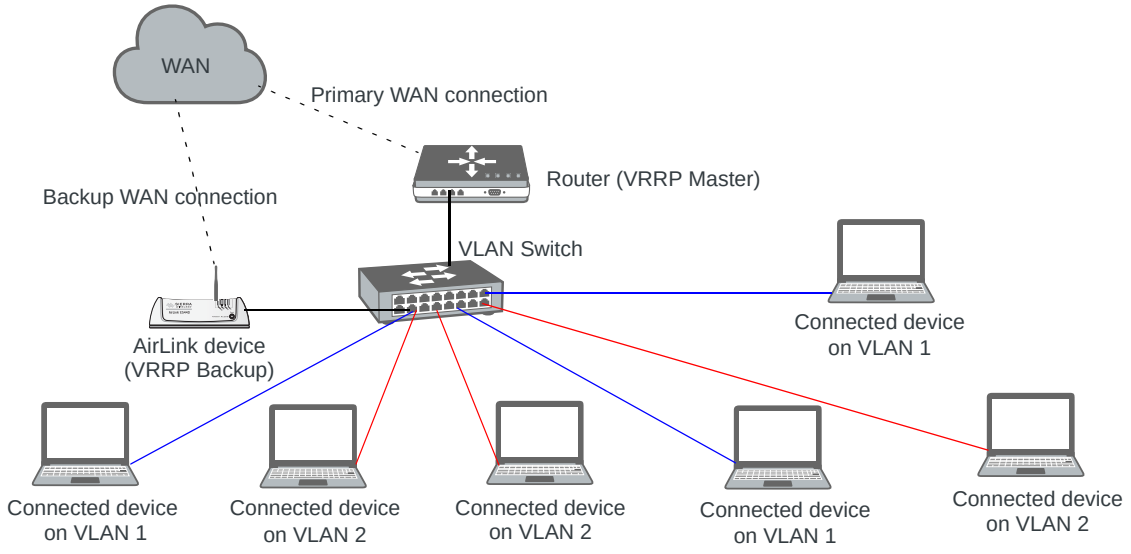


Figure 5-34: VRRP Network Configuration with VLANs

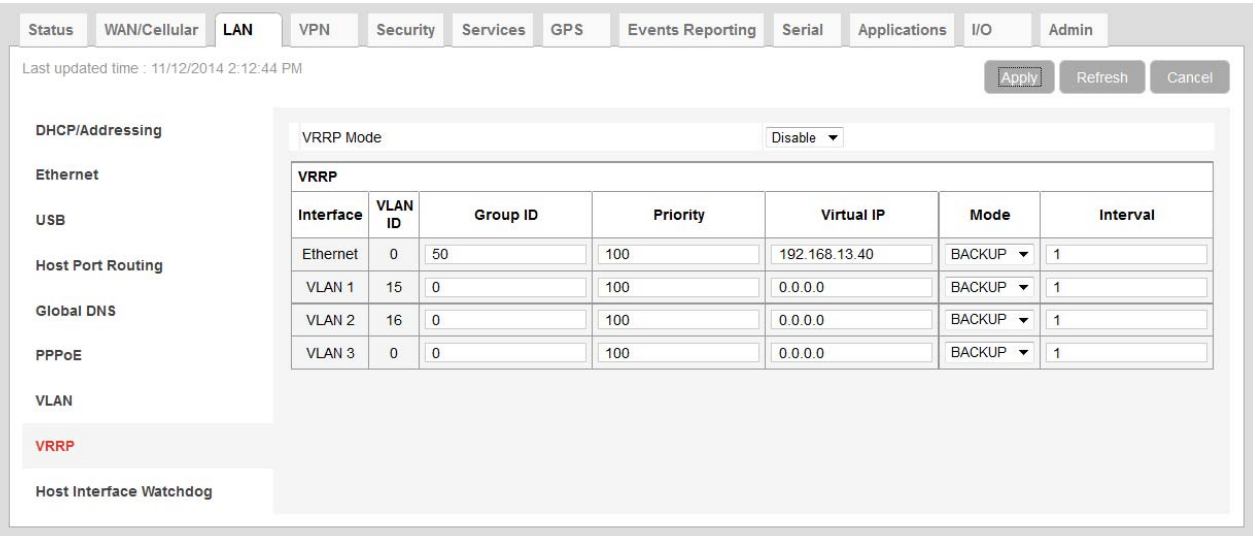


Figure 5-35: ACEmanager: LAN > VRRP (no VLANs)

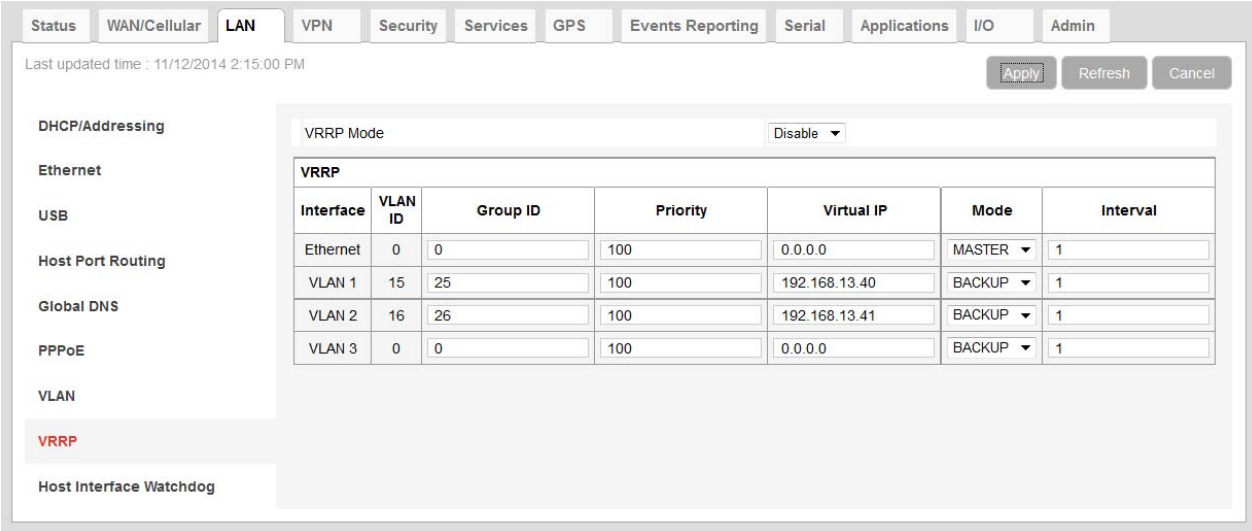


Figure 5-36: ACEmanager: LAN > VRRP (VLANs)

You can also set up VRRP using two AirLink devices—one configured as the VRRP Master and the other as the VRRP Backup. The Backup AirLink device provides an alternate route when the Master AirLink device loses coverage.

For example, if you have cellular accounts with two different Mobile Network Operators (MNOs) you might prefer to use MNO A's connection, but to maintain continuity, you would like traffic to switch to MNO B if A's network is down and switch back to A's network once the connection is re-established, as shown in Figure 5-37.

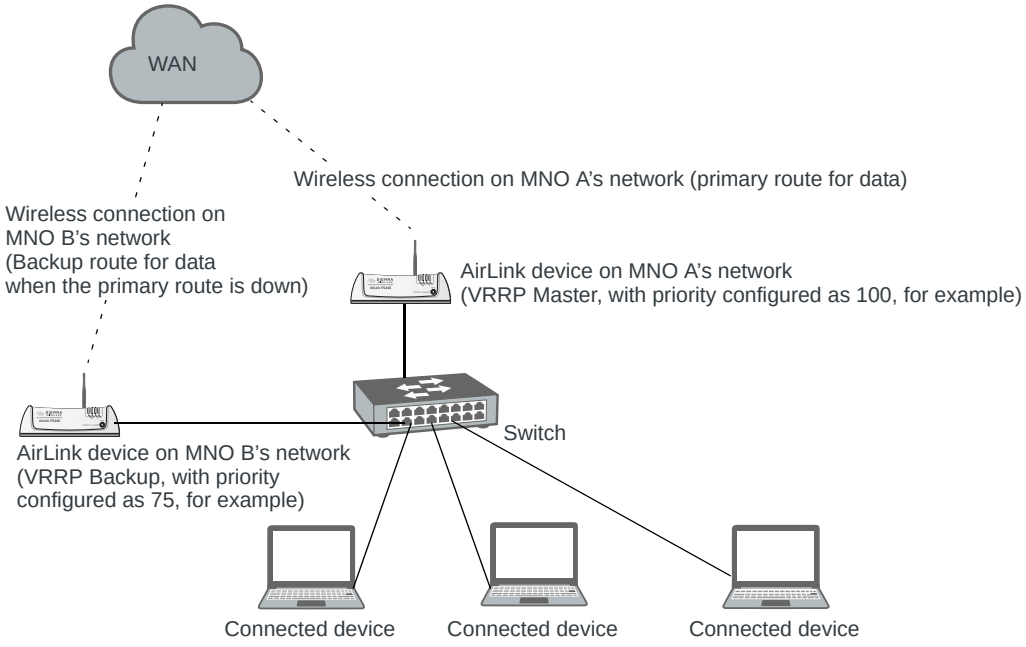

WAN
Wireless connection on MNO A's network (primary route for data)
Wireless connection on MNO B's network (Backup route for data when the primary route is down)
AirLink device on MNO A's network (VRRP Master, with priority configured as 100, for example)
Switch
AirLink device on MNO B's network (VRRP Backup, with priority configured as 75, for example)
Connected device
Connected device
Connected device

Figure 5-37: VRRP Network Configuration using two AirLink devices

Field	Description
VRRP Enabled	Allows you to activate VRRP. Options are: • Enable • Disable (default)
VRRP — The VLAN ID, Group ID, and Virtual IP address must be the same on the VRRP Master and VRRP Backup devices.	
Interface	Displays Ethernet port on AirLink device and the VLAN numbers
VLAN ID	Displays the VLAN ID This value is inherited from the LAN > VLAN screen. (See VLAN on page 146.) • 0—VLAN is disabled • 1–4094—Valid range for VLAN ID
Group ID	Enter the VRRP Group ID. Configure the VRRP Master (for example, the 3rd party router) and the VRRP Backup (for example the AirLink device) with the same Group ID. Options are: • 0–255 (Default is 0.)
Priority	Use this field to configure the priority for the AirLink device. The device with the highest priority (typically a 3rd party router) provides the primary data traffic route. If the device loses its connection to the WAN, its priority number drops. If the device fails, then when the failure is detected, the next highest priority router becomes the active router. The priority number configured on the VRRP Backup (typically the AirLink device) should be less than the initial priority number on the VRRP Master and greater than the value that the VRRP Master's priority number would be if it drops as a result of losing its WAN connection. For example, if the VRRP Master router has an initial priority number of 200 that drops to 80 if it loses its WAN connection, setting the AirLink device's priority to 100 ensures that it becomes the primary route if the VRRP Master loses its WAN connection. When the 3rd party router re-establishes its connection, its priority returns to 200 and it once again becomes the primary route for data. Options are: • 1–255 (Default is 100.)
Virtual IP	Configure the same virtual IP for the VRRP Backup (typically the AirLink device) and the VRRP Master (typically a 3rd party router). The virtual IP must be within the VLAN subnet.
Mode	Indicates the initial mode for the AirLink device Options are: • MASTER • BACKUP (default) *Note: Designating a device as "Master" in this field does not make it the primary route for data unless it is also given a higher priority number than the VRRP Backup device. See Priority.*
Interval	If the AirLink device is acting as VRRP Master, it advertises its Master status at the interval (in seconds) configured in this field. Options are: • 1–65535 seconds (Default value is 1.)

Host Interface Watchdog

The Host Interface Watchdog provides a way for you to ensure that the LAN connection is alive. You can use this feature to monitor:

- A host connected to the LAN via an Ethernet or USB connection
- A host computer associated with a GX Series device that has a Wi-Fi X-Card installed, provided the Wi-Fi mode is set to “Access Point” or “Both” (See Wi-Fi on page 129.)

When the Host Interface Watchdog is enabled, ALEOS sends a ping to the connected host at configured intervals. You can disable Force Keepalive to only send a ping when there is no traffic on the LAN interface. (See Force LAN Keepalive on page 153.)

If there is no response to the ping, the LAN interface is reset.

Note: The network interface is automatically determined from the IP address and the LAN configuration. If you have multiple interfaces bridged (see Bridge Wi-Fi to Ethernet on page 115) all interfaces in the bridge and the bridge itself are reset.

After the interface comes back up, ALEOS sends another ping to the connected host. If there is still no response to this ping, the AirLink device reboots. After a reboot caused by the LAN Interface Watchdog, ALEOS waits an hour before attempting pings to prevent repeated frequent reboots.

Note: DUN (PPP) is not supported. If the IP address for the host is on a DUN network, the feature is disabled.

Note: The feature is not disabled when the interface uses Public Mode, but it cannot monitor the host interface unless the cellular network provides a static IP.

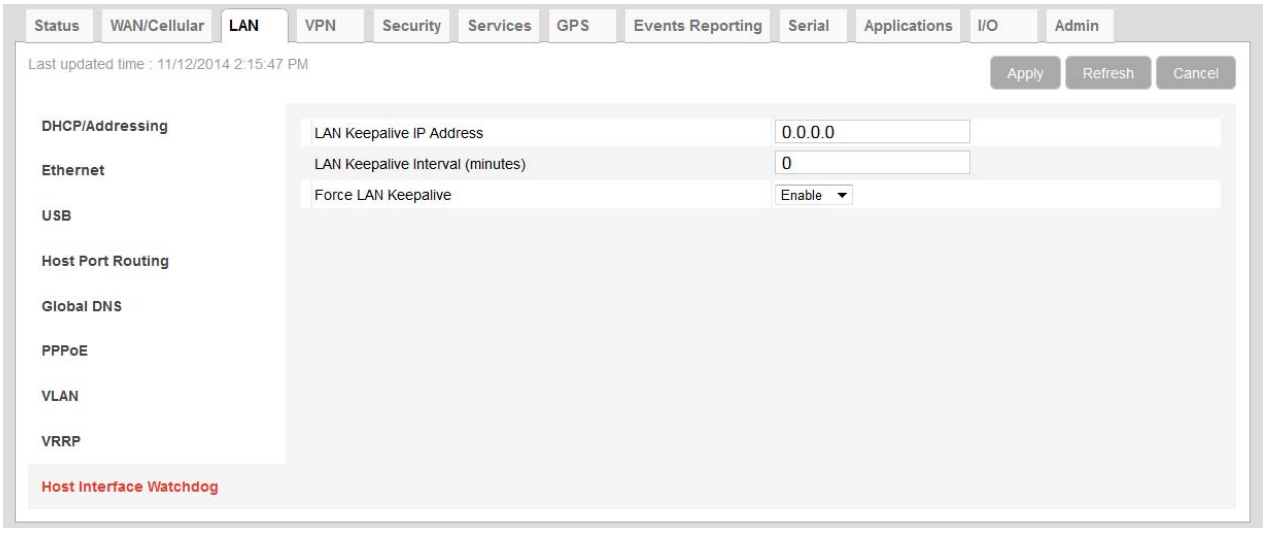


Figure 5-38: ACEmanager: LAN > Host Interface Watchdog

Field	Description
LAN Keepalive IP address	Enter the IP address of the host to ping If a host IP address is not configured, the Host Interface Watchdog is disabled.
LAN Keepalive Interval (minutes)	The interval (in minutes) at which ALEOS pings the LAN-connected device Options are: 1–1440 If this field is set to 0, the Host Interface Watchdog is disabled. (default) To prevent the device from rebooting frequently when a connection is not available, if the device reboots as a result of a failed keepalive ping, it waits 60 minutes before sending another keepalive ping. Once the ping is successful, the device returns to the interval configured in this field.
Force LAN Keepalive	• Enabled (default)—The network interface statistics are not monitored and a ping is always sent at the interval configured in the Keepalive Interval field. • Disabled—The network interface statistics are monitored and connectivity is assumed when there is traffic received. A ping is only sent when there is no traffic for a period greater than the interval set in the Keepalive Interval field.

6: VPN Configuration

6

The AirLink device can act as a Virtual Private Network (VPN) device, providing enterprise VPN access to any device connected to the AirLink device even when a device has no VPN client capability on its own. The AirLink device supports three types of VPN: IPsec, GRE, and SSL. The AirLink device can support up to five VPN tunnels at the same time.

Note: Dynamic Mobile Network Routing (DMNR) is not compatible with VPN tunnels. If you are using DMNR, disable all VPN tunnels.

IPsec

The IP protocol that drives the Internet is inherently insecure. Internet Protocol Security (IPsec), which is a standards-based protocol, secures communications of IP packets over public networks.

IPsec is a common network layer security control and is used to create a virtual private network (VPN).

The advantages of using the IPsec feature includes:

- Data Protection: Data Content Confidentiality allows you to protect your data from any unauthorized view, because the data is encrypted (encryption algorithms are used).
- Access Control: Access Control implies a security service that prevents unauthorized use of a Security Gateway, a network behind a gateway or bandwidth on that network.
- Data Origin Authentication: Data Origin Authentication verifies the actual sender, thus eliminating the possibility of forging the actual sender's identification by a third-party.
- Data Integrity: Data Integrity Authentication allows both ends of the communication channel to confirm that the original data sent has been received as transmitted, without being tampered with in transit. This is achieved by using authentication algorithms and their outputs.

Split Tunnel

The AirLink device supports Global settings with one encrypted tunnel and one open tunnel. A sample server subnet for a Global setting would be 172.16.1.0/24. Global settings VPNs should be set up with care, as a Global settings configuration with both an enterprise VPN and access to the public Internet can inadvertently expose company resources.

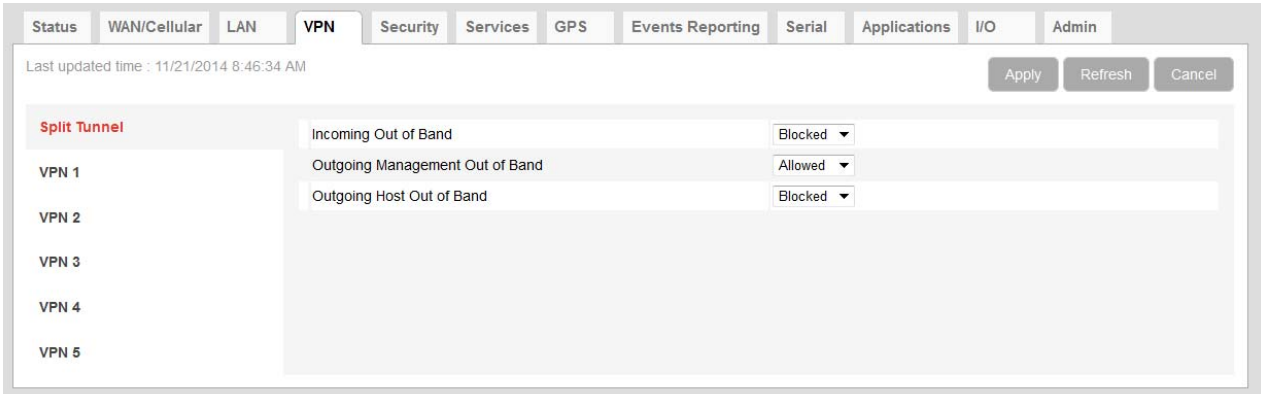


Figure 6-1: ACEmanager: VPN > Split Tunnel

Field	Description
Incoming Out of Band	Controls incoming public Internet traffic Options are: • Blocked—Incoming public Internet traffic is blocked. Only traffic through the VPN tunnel is allowed. (default) • Allowed—Incoming public Internet traffic is allowed.
Outgoing Management Out of Band	Controls outgoing traffic from the AirLink device • Blocked—Outgoing traffic from the AirLink device to the public Internet is blocked. Only traffic through the VPN tunnel is allowed. • Allowed—Outgoing traffic from the AirLink device to the public Internet is allowed. (default)
Outgoing Host Out of Band	Controls of outgoing Host out of band traffic. Options are: • Blocked—Public Internet traffic from the host device is blocked. Only traffic through the VPN tunnel is allowed. (default) • Allowed—Public Internet traffic from the host device is allowed.

VPN 1

The VPN 1 tunnel can be configured as IPsec, GRE, or SSL. Enabling any of these tunnels will expose other options for configuring the tunnel.

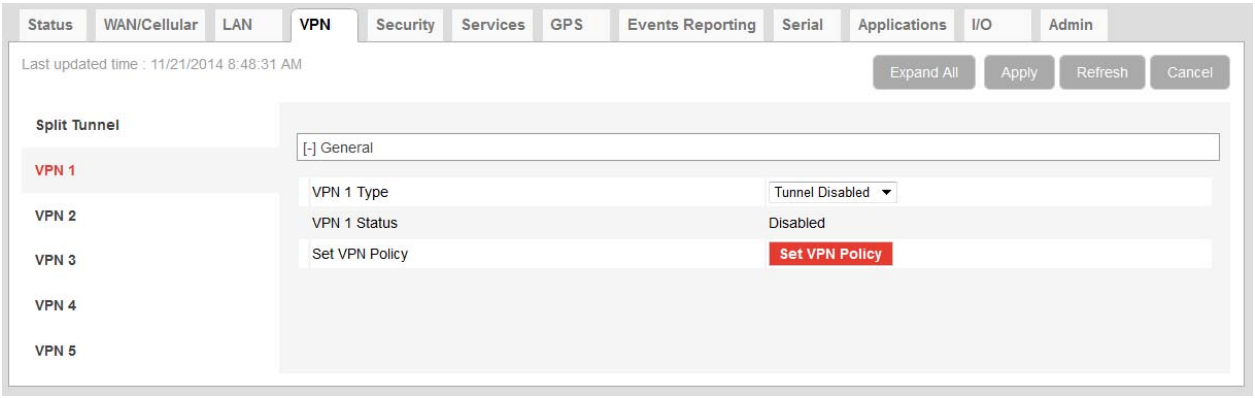


Figure 6-2: ACEmanager: VPN > VPN 1

IPsec

The IPsec architecture model includes the Sierra Wireless AirLink gateway as a remote gateway at one end communicating, through a VPN tunnel, with a VPN gateway at the other end. The remote gateway is connected to a Remote network and the VPN is connected to the Local network. You can configure up to three remote subnets. The communication of data may be secured through the use of IPsec protocols.

The IPsec VPN employs the IKE (Internet Key Exchange) protocol to set up a Security Association (SA) between the AirLink device and a Cisco (or Cisco compatible) enterprise VPN server. IPsec consists of two phases to set up an SA between peer VPNs. Phase 1 creates a secure channel between the AirLink Device VPN and the enterprise VPN, thereby enabling IKE exchanges. Phase 2 sets up the IPsec SA that is used to securely transmit enterprise data.

You can specify either or both peers—local (My Identity Type field) and remote (Peer Identity Type field) using an FQDN (Fully Qualified Domain Name) or the IP address.

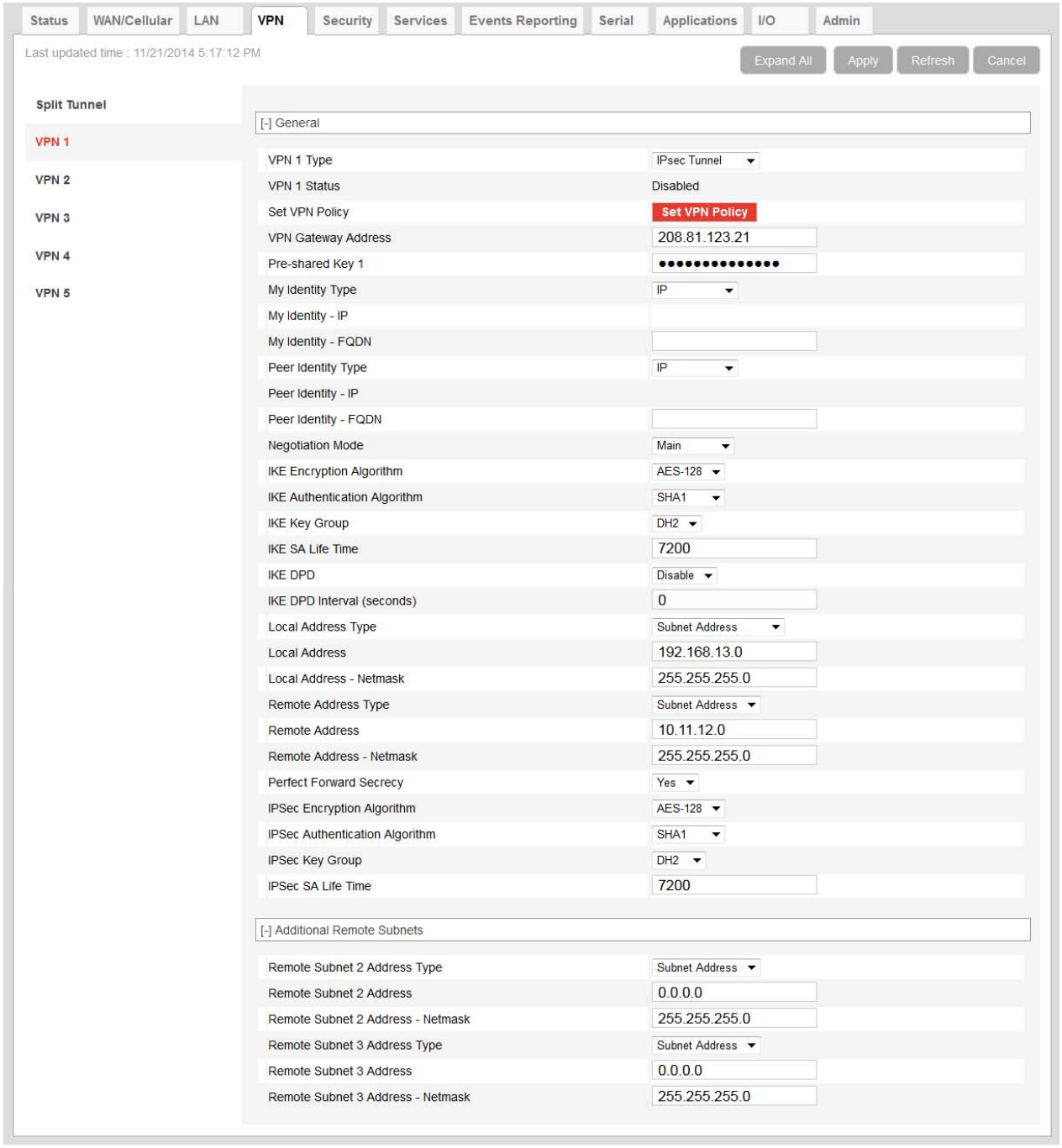


Figure 6-3: ACEmanager: VPN > VPN 1 > IPsec Tunnel

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td colspan="2">General</td></tr>
<tr><td>VPN # Type</td><td>Use this field to enable or disable the VPN # tunnel. If custom settings are used, they will be saved and the tunnel can be disabled and re-enabled without needing to reenter any of the settings. For a successful configuration, all settings for the VPN tunnel must be identical between the AirLink Device VPN and the enterprise VPN server.
Options are:
• Tunnel Disabled (default)
• IPsec Tunnel
• GRE Tunnel
• SSL Tunnel</td></tr>
<tr><td>VPN # Status</td><td>Indicates the current status of the VPN # connection. Use this when troubleshooting a VPN # connection. Options are: Disabled, Not Connected, or Connected.</td></tr>
<tr><td>Set VPN Policy</td><td>Click this button to apply the new settings. The device does not need to be rebooted.</td></tr>
<tr><td>VPN Gateway Address</td><td>The IP address or FQDN (Fully Qualified Domain Name) of the server that this VPN client connects to. This address must be open to connections from the AirLink device. The default VPN Gateway IP Addresses are static address on Sierra Wireless Servers. They are:
<table><tr><th>VPN</th><th>Gateway IP Address</th></tr><tr><td>1</td><td>208.81.123.21</td></tr><tr><td>2</td><td>208.81.123.22</td></tr><tr><td>3</td><td>208.81.123.26</td></tr><tr><td>4</td><td>208.81.123.23</td></tr><tr><td>5</td><td>208.81.123.24</td></tr></table>You can use these default IP addresses to confirm that an IPSec connection can be established with your wireless configuration before making any configuration changes, and as an example to model your VPN configuration after. (See Figure 6-3.)</td></tr>
<tr><td>Pre-shared Key 1</td><td>Pre-shared Key (PSK) used to initiate the VPN tunnel</td></tr>
<tr><td>My Identity Type</td><td>Options are:
• IP (default) — The My Identity - IP field appears with the WAN IP address assigned by the carrier
• FQDN — The My Identity - FQDN field appears. Enter a fully qualified domain name (FQDN) e. g., modemname.domainname.com
• User FQDN — The My Identity - FQDN field appears. Enter a User FQDN whose values should include a username (e.g. user@domain.com)</td></tr>
</table>

Field	Description
My Identity - IP or **My Identity - FQDN**	• My Identity - IP appears only when IP is selected from the My Identity Type drop-down menu. The WAN IP address assigned by the carrier appears. • My Identity - FQDN appears only when User FQDN or FQDN is selected from the My Identity Type drop-down menu. Enter an FQDN or User FQDN. *Note: If you are using a FQDN for your device (My Identity) either:* • *Set up a Dynamic DNS on the Services > Dynamic DNS tab. (See Dynamic DNS on page 191.) or* • *Use a DNS server as your domain host*
Peer Identity Type	Required in some configurations to identify the client or peer side of a VPN connection. Options are: • IP (default) — The Peer Identity - IP field appears with the IP address of a VPN server set up by Sierra Wireless for your testing purposes • FQDN — The Peer Identity - FQDN field appears. Enter an FQDN (e. g. modemname.domainname.com) • User FQDN — The Peer Identity - FQDN field appears. Enter a User FQDN whose values should include a username (e.g., user@domain.com)
Peer Identity - IP or **Peer Identity - FQDN**	• Peer Identity - IP appears only when IP is selected from the Peer Identity Type drop-down menu. The VPN Gateway IP Address appears. • Peer Identity - FQDN appears only when User FQDN or FQDN is selected from the Peer Identity Type drop-down menu. Enter the Peer FQDN or Peer User FQDN.
Negotiation Mode	Enable this configuration to operate the onboard VPN under Aggressive mode. Aggressive mode offers increased performance at the expense of security. Options are: • Main (default) • Aggressive
IKE Encryption Algorithm	Determines the type and length of encryption key used to encrypt/decrypt ESP (Encapsulating Security Payload) packets. 3DES supports 168-bit encryption. AES (Advanced Encryption Standard) supports both 128-bit and 256-bit encryption. Options are: DES, 3DES, AES-128 (default), and AES-256
IKE Authentication Algorithm	MD5 is an algorithm that produces a 128-bit digest for authentication. SHA is a more secure algorithm that produces both 160-bit (SHA1) and 256-bit (SHA256) digests. Options are: MD5, SHA1 (default), and SHA256
IKE Key Group	Options are: DH1, DH2 (default), or DH5
IKE SA Life Time	Determines how long the VPN tunnel is active in seconds. Options are: 180 to 86400; Default: 7200

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>IKE DPD</td><td>Dead Peer Detection (DPD)
Options are:
Disable (default)
Enable
When DPD is enabled, the AirLink device checks to see if the server is still present if there has been no traffic for a configured interval. If it does not receive an acknowledgment, it retries at 5 second intervals. If there is no acknowledgment after 5 retries, the status of the VPN is set to Not Connected and the device attempts to renegotiate IPSEC security parameters with its peer.
Default is Disabled.

Note: Sierra Wireless recommends that you Enable IKE DPD. Otherwise the AirLink device has no way of detecting that the connection to the VPN server is still available.</td></tr>
<tr><td>IKE DPD Interval (seconds)</td><td>Use this field to set the DPD interval (in seconds). If there has been no traffic for the period of time set in this field, the AirLink device retries checking with the server, as described in IKE DPD.
Options are: 0 to 3600 (default is 1200)
If this field is set to 0, DPD monitoring is turned off (or disabled as described in the IKE DPD section), but the AirLink device still responds to DPD requests from the server.</td></tr>
<tr><td>Local Address Type</td><td>The network information of the device. Options are: Use the Host Subnet, Single Address, and Subnet Address (default)</td></tr>
<tr><td>Local Address</td><td>Device subnet address</td></tr>
<tr><td>Local Address - Netmask</td><td>Device subnet mask information; 24-bit netmask
Default: 255.255.255.0</td></tr>
<tr><td>Remote Address Type</td><td>The network information of the IPsec server behind the IPsec gateway.
Options are: Subnet Address (default) and Single Address</td></tr>
<tr><td>Remote Address</td><td>The IP address or subnet of the device(s) connected to the gateway
This value cannot be 0.0.0.0
Default values are:

<table><tr><th>VPN</th><th>Remote Address</th></tr><tr><td>1</td><td>10.11.12.0</td></tr><tr><td>2</td><td>10.11.13.0</td></tr><tr><td>3</td><td>10.11.14.0</td></tr><tr><td>4</td><td>10.11.15.0</td></tr><tr><td>5</td><td>10.11.16.0</td></tr></table></td></tr>
<tr><td>Remote Address - Netmask</td><td>Remote subnet mask information. 24-bit netmask
Default: 255.255.255.0</td></tr>
</table>

Field	Description
Perfect Forward Secrecy	Provides additional security through a DH shared secret value. When this feature is enabled, one key cannot be derived from another. This ensures previous and subsequent encryption keys are secure even if one key is compromised. Options are: Yes (default) or No.
IPsec Encryption Algorithm	Determines the type and length of encryption key used to encrypt/decrypt ESP (Encapsulating Security Payload) packets. 3DES supports 168-bit encryption. AES (Advanced Encryption Standard) supports both 128-bit and 256-bit encryption. Options are: None, DES, 3DES, AES-128 (default), and AES-256.
IPsec Authentication Algorithm	Can be configured with MD5 or SHA1. MD5 is an algorithm that produces a 128-bit digest for authentication. SHA is a more secure algorithm that produces both 160-bit (SHA1) and 256-bit (SHA256) digests. Options are: None, MD5, SHA1 (default), and SHA 256.
IPsec Key Group	Determines how the AirLink Device VPN creates an SA with the VPN server. The DH (Diffie-Hellman) key exchange protocol establishes pre-shared keys during the phase 1 authentication. The AirLink Device supports three prime key lengths, including Group 1 (768 bits), Group 2 (1,024 bits), and Group 5 (1,536 bits). Options are: None, DH1, DH2 (default), or DH5.
IPsec SA Life Time	Determines how long the VPN tunnel is active in seconds Options are: 180 to 86400; Default: 7200
Additional Remote Subnets	
Remote Subnet 2 Address type	The network information for subnet 2 IPsec server behind the IPsec gateway. Options are: Subnet Address (default) and Single Address
Remote Subnet 2 Address	The IP address for the subnet 2 device behind the gateway
Remote Subnet 2 Address - Netmask	Remote subnet 2 mask information. 24-bit netmask Default: 255.255.255.0
Remote Subnet 3 Address type	The network information for subnet 3 IPsec server behind the IPsec gateway. Options are: Subnet Address (default) and Single Address
Remote Subnet 3 Address	The IP address for the subnet 3 device behind the gateway
Remote Subnet 3 Address - Netmask	Remote subnet 3 mask information. 24-bit netmask Default: 255.255.255.0

GRE

The AirLink Device can act as a Generic Routing Encapsulation (GRE) endpoint, providing a means to encapsulate a wide variety of network layer packets inside IP tunneling packets. With this feature you can reconfigure IP architectures without worrying about connectivity. GRE creates a point-to-point link between routers on an IP network.

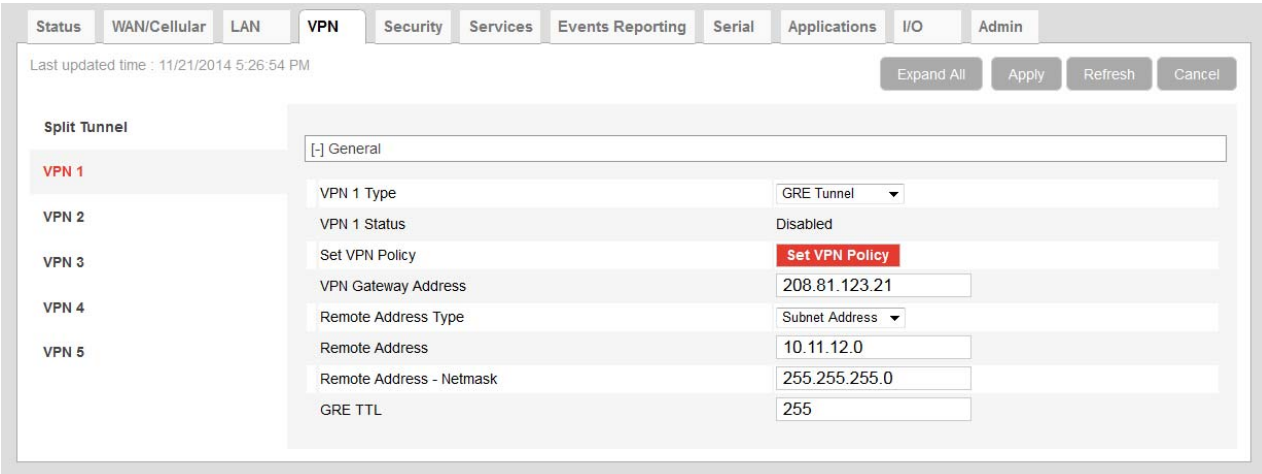


Figure 6-4: ACEmanager: VPN > VPN1 > GRE Tunnel

See the IPsec table for parameter descriptions.

Field	Description
VPN # Type	Options are: Tunnel Disabled or GRE Tunnel. Enabling the GRE Tunnel will expose other options for configuring the tunnel.
VPN # Status	Indicates the status of the GRE tunnel on the device Options are: Disabled, Connected or Not Connected
Set VPN Policy	Click this button to apply the new settings. The device does not need to be rebooted.
VPN Gateway Address	The IP address of the device that this client connects to. This IP address must be open to connections from the device.
Remote Address Type	The network information of the GRE server behind the GRE gateway
Remote Address	The IP address of the device behind the gateway
Remote Address - Netmask	The subnet network mask of the device behind the GRE gateway *Note: Never use a 16-bit subnet mask: GRE tunnel establishment will fail.*
GRE TTL	GRE time to live (TTL) value is the upper bound on the time that a GRE packet can exist in a network. In practice, the TTL field is reduced by one on every router hop. This number is in router hops and not in seconds.

SSL Tunnel

The SSL tunnel allows the device and the server to communicate across a network securely. SSL provides endpoint authentication and secure communications over the Internet.

If the SSL tunnel is selected, you can opt to secure remote communications via SSL.

The AirLink device client will authenticate the server using a PKI certificate. The server will authenticate the client via username and password. The Root CA certificate for the server certificate must be loaded on the device.

Note: SSL tunnel is based on the OpenVPN open source package. AirLink devices are SSL clients and will only talk to an SSL server (also based on the OpenVPN package).

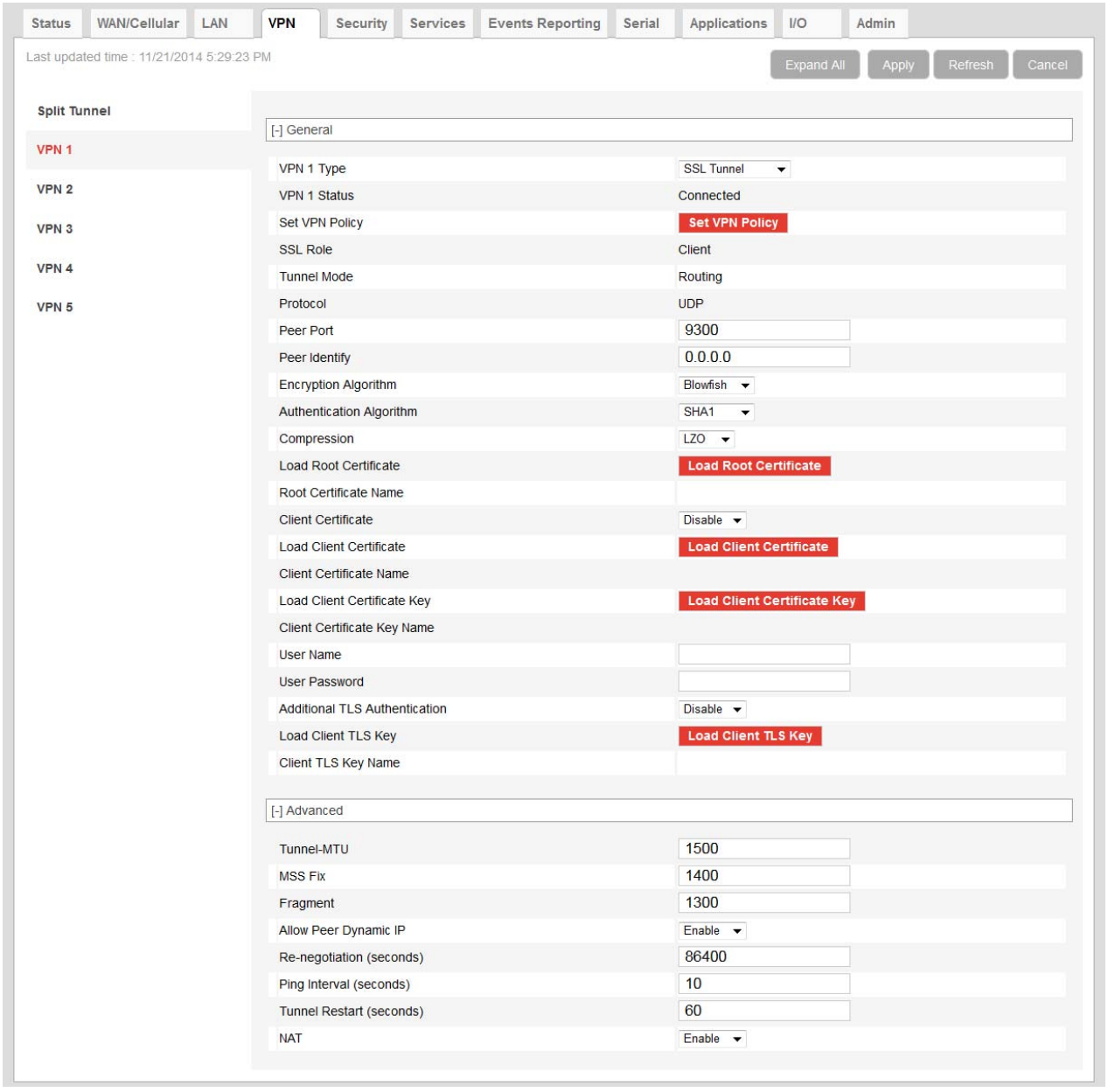


Figure 6-5: ACEmanager: VPN > VPN1 > SSL Tunnel

Field	Description
General	
VPN 1 Type	Options are: Tunnel Disabled or SSL Tunnel. Enabling the SSL Tunnel will expose other options for configuring the tunnel.
VPN 1 Status	Indicates the status of the SSL tunnel on the device Options are: Disabled, Connected or Not Connected
Set VPN Policy	Click this button to apply the new settings. The device does not need to be rebooted.
SSL Role	The AirLink device can only be an SSL client. Default: Client
Tunnel Mode	The Tunnel Mode is set to “Routing”.
Protocol	Displays the protocol used for configuration. Only supports UDP
Peer Port	The Peer Port is the UPD port on the peer device.
Peer Identity	Enter the IP address or Fully Qualified Domain Name (FQDN) of the peer device.
Encryption Algorithm	Options are: DES, Blowfish, DES, Cast128, AES-128, and AES-256
Authentication Algorithm	Options are: MD5, SHA-1, and SHA-256
Compression	Options are: LZ0 or NONE
Load Root Certificate	Loads the server root CA (Certificate Authority) certificate When you click the button, a window pops up and enables you to browse and select the file containing the root CA certificate.
Root Certificate Name	Displays the name of the most recently uploaded root certificate
Client Certificate	Enables or disables use of a client certificate.
Load Client Certificate	This field appears only if Client Certificate is enabled. Loads the client certificate When you click the button, a window pops up and enables you to browse and select the file containing the client certificate.
Client Certificate Number	Displays the number of the most recently uploaded client certificate.
Load Client Certificate Key	This field appears only if Client Certificate is enabled. Loads the client certificate key When you click the button, a window pops up and enables you to browse and select the file containing the client certificate key.
Client Certificate Key Name	Displays the name of the most recently uploaded client certificate key
User Name	The user name required for client authentication
User Password	The user password required for client authentication
Additional TLS Authentication	Enables or disables use of Transport Layer Security (TLS) authentication.

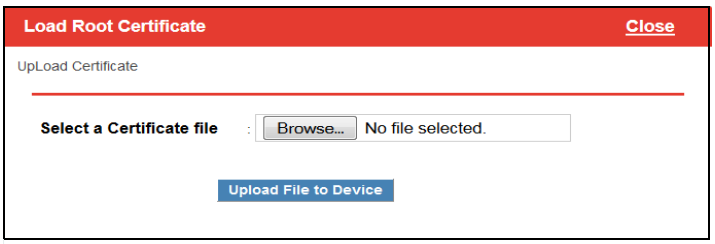
Field	Description
Load Client TLS Key	This field appears only if Additional TLS Authentication is enabled. Loads the client TLS key When you click the button, a window pops up and enables you to browse and select the file containing the client TLS key.
Client TLS Key Name	Displays the name of the most recently uploaded client TLS key
Advanced	
Tunnel-MTU	Default: 1500 bytes
MSS Fix	Default: 1400 bytes
Fragment	Default: 1300 bytes
Allow Peer Dynamic IP	Options are: Enable or Disable
Re-negotiation (seconds)	Default: 86400 (24 hours)
Ping Interval (seconds)	This is the keep-alive sent by the client. Default: 0 seconds
Tunnel Restart (seconds)	Enter the time for a tunnel restart (unit in seconds)
NAT	Options are: Enable or Disable. Note that this is a Carrier NAT, not a local NAT

Load Root Certificate

Note: The process is similar for uploading the client certificate, the client certificate key and the client TLS key.

To load a root certificate:

1. Click Load Root Certificate.
   The following dialog-box appears.



2. Select the appropriate file for your device.
3. Click Upload File to Device.

VPN 2 to VPN 5

The VPN 2 through VPN 5 sections only allow configuration of the IPsec and GRE tunnels on the device. Figure 6-3 shows the screen display for the VPN 2 submenu; screen data fields for the VPN 3, 4, and 5 submenus are identical.

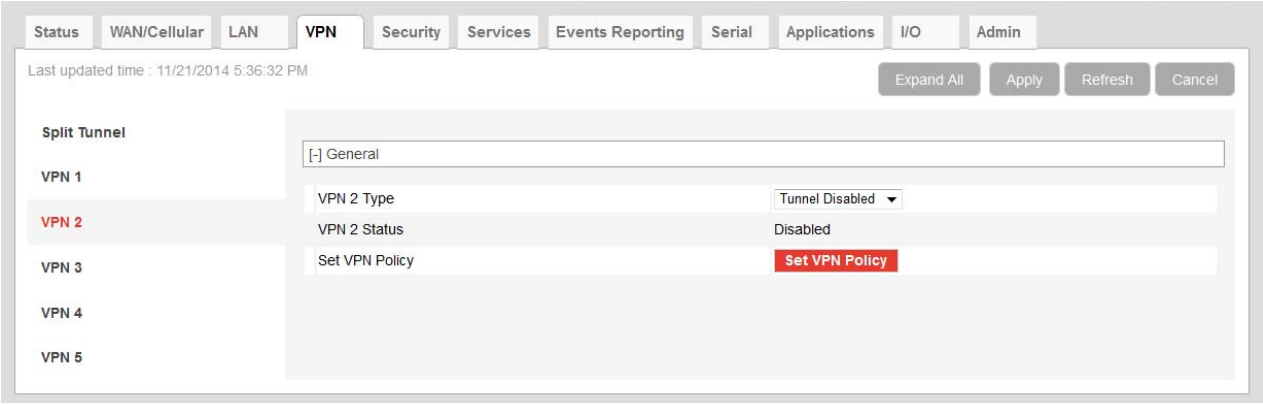


Figure 6-6: ACEmanager: VPN > VPN 2

There are three options in the scroll down menu: Tunnel Disabled, IPsec Tunnel, and GRE Tunnel. Enabling the IPsec or GRE Tunnel will expose other options for configuring that tunnel. The options shown for VPN 1 on page 157 are the same for VPNs 2 through 5.

Field	Description
VPN 2 Type	Options are: • Tunnel Disabled • IPSec Tunnel • GRE Tunnel

7: Security Configuration

7

The security tab covers firewall-type functions. These functions include how data is routed or restricted from one side of the device to the other, i.e., from computers or devices connected to the device (LAN) and from computers or devices contacting it from a remote source (WAN). These features are set as rules.

Tip: *For additional security, Sierra Wireless recommends that you change the default password for ACEmanager. See* *Change Password on page 325.*

Solicited vs. Unsolicited

How the device responds to data being routed from one network connection to the other depends on the origin of the data.

- If a computer on the LAN initiates a contact to a WAN location (such as a LAN connected computer accessing an Internet web site), the response to that contact is solicited.
- If, however, a remote computer initiates the contact (such as a computer on the Internet accessing a camera connected to the device), the connection is considered unsolicited.

Port Forwarding

In Port Forwarding, any unsolicited data coming in on a defined Public Port is routed to the corresponding Private Port and Host IP of a device connected to the specified Physical Interface. You can forward a single port or a range of ports.

Note: Port Forwarding requires Private Mode. See *Private and Public Mode on page 111.*

Figure 7-1: Port Forwarding

Single port

To define a port forwarding rule for a single port:

1. In ACEmanager, go to Security > Port Forwarding.

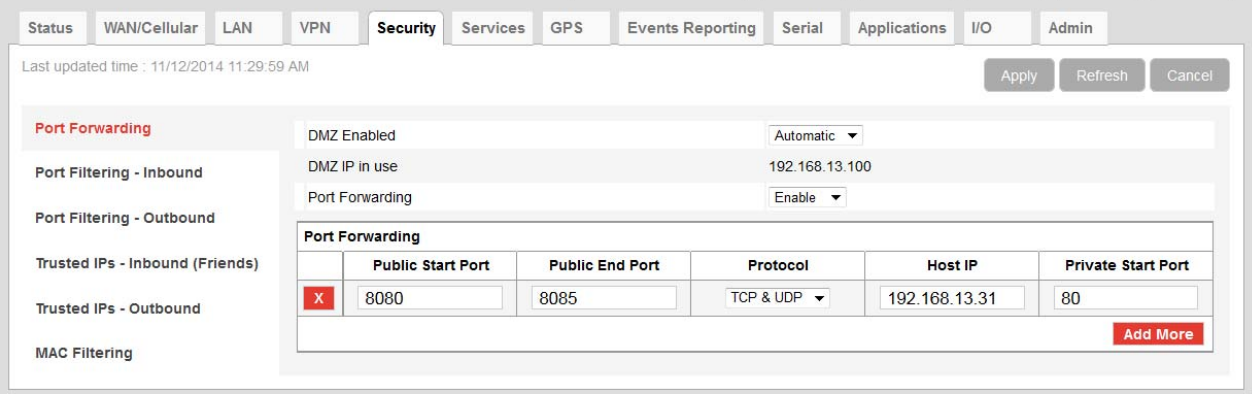


Figure 7-2: ACEmanager: Security > Port Forwarding (Single Port)

2. In the Port Forwarding field, select Enable.
3. Click “Add More” to display a rule line.
4. In the Public Start Port field, enter the desired public network port number. Values between 1 and 65535 are supported, although Sierra Wireless recommends using a value greater than 1024.

   Unsolicited data coming in on this port is forwarded to the port you select in the Private Start Port field.
5. In the Public End Port field, enter 0.
6. Select the desired protocol (see Protocol on page 172):
   - TCP
   - UDP
   - TCP & UDP
7. Enter the IP address of the computer you want to forward data to.
8. In the Private Start Port field, enter the number of the port on the destination computer that you want to forward data to.
9. Click Apply.
10. Reboot.

    You do not need to reboot immediately, if you have additional changes to make, but port forwarding does not take effect until the device is rebooted.

Range of ports

To define a port forwarding rule for a range of ports:

1. In ACEmanager, go to Security > Port Forwarding.

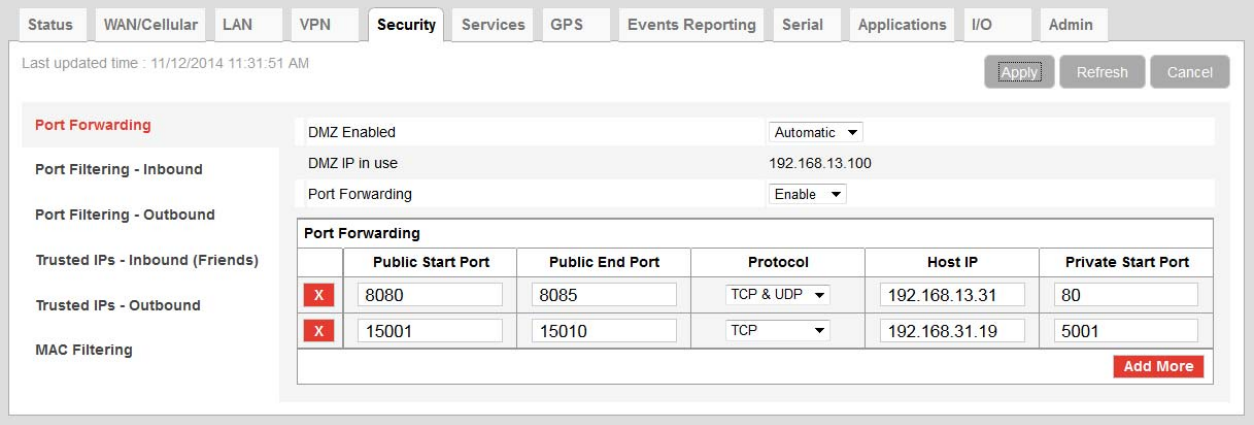


Figure 7-3: ACEmanager: Security > Port Forwarding (Port Range)

2. In the Port Forwarding field, select Enable.
3. Click “Add More” to display a rule line.
4. Set the port range for incoming data:
   a. In the Public Start Port field, enter the desired public network port number. Values between 1 and 65535 are supported, although Sierra Wireless recommends using a value greater than 1024.
   b. In the Public Port End field, enter the last public network port number in the range. The value you enter in the Public Port End field must be greater than the value in the Public Start Port field, or ALEOS rejects the selection.

      Unsolicited data coming in on ports in this range are forwarded to a range of ports, starting with the port you select in the Private Start Port field.
5. Select the desired protocol (see Protocol on page 172):
   - TCP
   - UDP
   - TCP & UDP
6. Enter the IP address of the computer you want to forward data to.

   To forward a port to a local ALEOS Service, set the Host IP to 127.0.0.1.
7. In the Private Start Port field, enter the starting port number for the range of ports on the destination computer that you want to forward data to.
8. Click Apply.
9. Reboot.

   You do not need to reboot immediately, if you have additional changes to make, but port forwarding does not take effect until the device is rebooted.

Note: Sierra Wireless recommends that the total number of port forwardings be fewer than 1000 ports, including single port forwarding and port forwarding within a range.

Field	Description
Port Forwarding	Enables port forwarding rules. Options are Enable and Disable (default).
Public Start Port	Port on the public network or starting port on the public network for a range of ports. • Supported values: 1–65535 (Recommended values: greater than 1024)
Public End Port	Ending port for a range of ports on the public network. • For a single port forwarding, this field must be 0. • For a range of ports, this value must be greater than the value in the Public Start Port field.
Protocol	The protocol to be used with the forwarded port: • TCP—Only those unsolicited data requests using TCP are forwarded • UDP—Only those unsolicited data requests using UDP are forwarded • TCP & UDP—Unsolicited data requests using either TCP or UDP are forwarded
Host IP	IP address of the computer (or device) you want to forward data to.
Private Start Port	Port on the destination computer used as the port for single port forwarding rules, or as the start port for a port forwarding range.

Port Forwarding Example

The following example shows you how to configure a port forward rule for a range of 6 ports on an Ethernet-connected device:

1. In ACEmanager, go to Security > Port Forwarding, and enable Port Forwarding.
2. Click “Add More” to display a rule line.
3. Enter 8080 for the Public Start Port.
4. Enter 8085 for the Public End Port.
5. Select TCP & UDP.
6. Enter 192.168.13.30 as the Host IP.
7. Enter 80 as the Private Start Port.

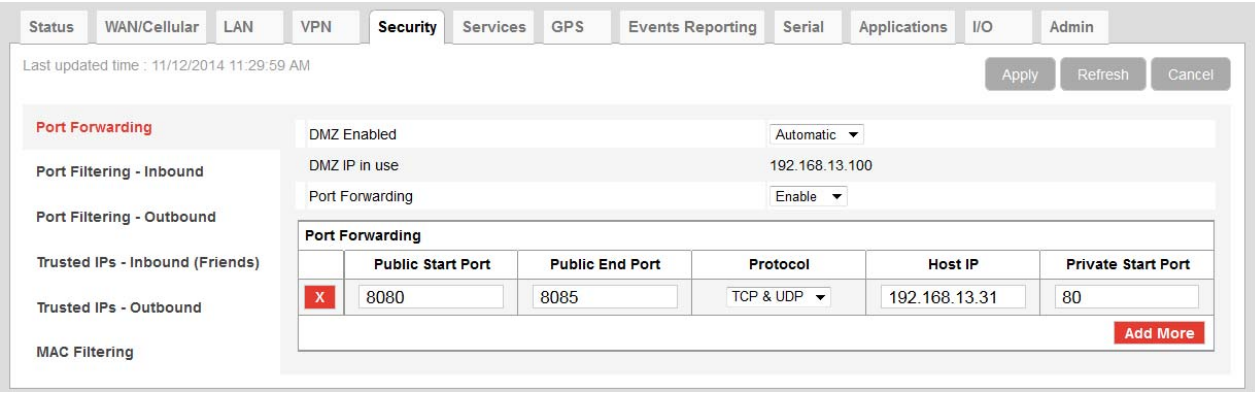


Figure 7-4: ACEmanager: Port Forwarding example

8. Click Apply.
9. Reboot.

   You do not need to reboot immediately, if you have additional changes to make, but port forwarding does not take effect until the device is rebooted.

An unsolicited TCP and UDP data request coming in to the AirLink device on port 8080 is forwarded to the LAN connected device, 192.168.13.30, at port 80. In addition, unsolicited data requests coming in from the Internet on ports 8081, 8082, 8083, 8084, and 8085 are forwarded to ports 81, 82, 83, 84, and 85 respectively.

DMZ

The DMZ is used to direct unsolicited inbound traffic to a specific LAN device such as a computer running a web server or other internal application. The DMZ with public mode is particularly useful for certain services like VPN, NetMeeting, and streaming video where the remote server may require a WAN connection to the LAN device rather than being NATed by the router. In public mode unsolicited traffic to hosts in the DMZ is permitted by default.

Options for DMZ are Automatic, Manual, and Disable.

Automatic uses the first connected host. If more than one host is available (multiple Ethernet on a switch connected to the device and/or Ethernet with USBnet) and you want to specify the host to use as the DMZ, select Manual and enter the IP address of the desired host.

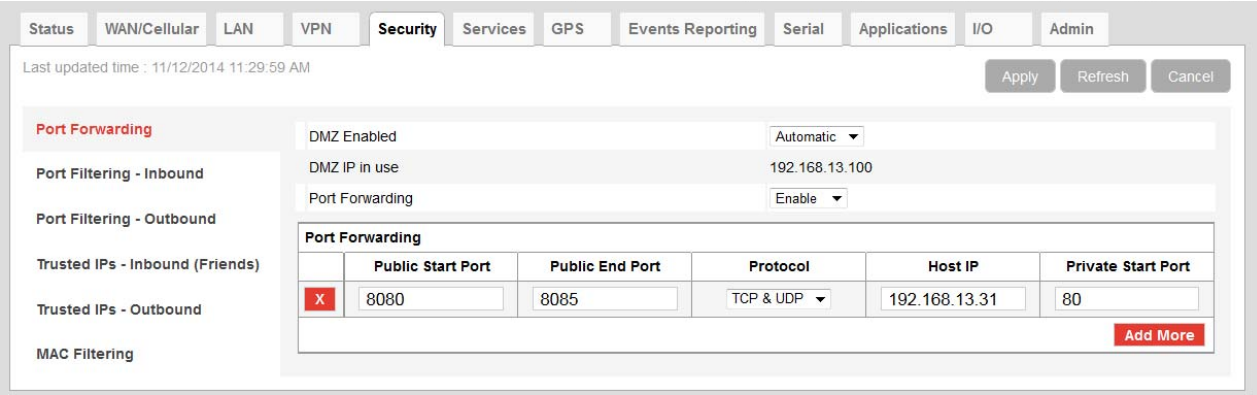


Figure 7-5: ACEmanager: Security > Port Forwarding (DMZ)

Field	Description
DMZ Enabled	The AirLink device allows a single client to connect to the Internet through a demilitarized zone (DMZ). Options are Automatic (default), Manual, and Disable. • Automatic—enables the first connected host or the Public Mode interface as the DMZ • Manual—inserts a specific IP address in the DMZ IP field • Disable—no connected host receives unsolicited traffic from the cellular network or Internet *Note: You can use a host connected to either Ethernet port on a Dual Ethernet X-Card as the host for Auto or Manual DMZ.*
DMZ IP	This field only appears if Manual is selected for the DMZ Enabled field; this field does not display if the DMZ is disabled. This is the IP address of the private mode host that should be used as the DMZ.
DMZ IP in use	IP address of the host to which inbound unsolicited packets are sent When the device passes the Network IP to the configured public host, the DMZ IP in Use displays the public IP.

Example of configuring the DMZ on an Ethernet connected device, using the settings shown in Figure 7-5:

1. Enter 192.168.13.100 for the DMZ IP.
2. Select Ethernet as the Default Interface.

An unsolicited data request coming in to the AirLink device on any port is forwarded to the LAN device, 192.168.13.100, at the same port.

Note: The DMZ settings are independent of the number of Port Forward entries and can be used with port forwarding to pass anything not forwarded to specific ports.

Port Filtering—Inbound

Port Filtering—Inbound restricts unsolicited access to the AirLink device and all LAN-connected devices.

You can enable Port Filtering to either block or allow specified ports. When enabled, all ports not matching the rule are allowed or blocked depending on the mode.

You can configure Port Filtering either on individual ports or for a range of ports. Click Add More for each port filtering rule you want to add.

Note: Inbound restrictions do not apply to responses to outbound data requests. To restrict outbound access, you need to set the applicable outbound filter.

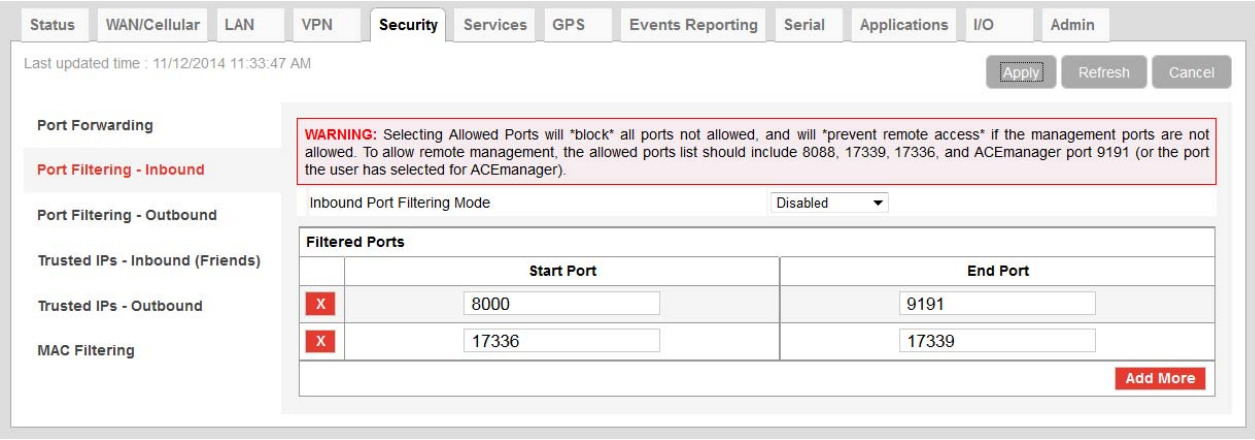


Figure 7-6: ACEmanager: Security > Port Filtering - Inbound

Field	Description
Inbound Port Filtering Mode	Options are: • Disable (default) • Blocked Ports—ports though which traffic is blocked (Shown in Filtered Ports list) • Allowed Ports—ports through which traffic is allowed (Shown in Filtered Ports list)
Filtered Ports	
Start Port	A single port or the first port in a range of ports on the public network (cellular network accessible)
End Port	The end of the range on the public network (cellular network accessible).

Warning: *Selecting Allowed Ports will *block* all ports not allowed, and will *prevent remote access* if the management ports are not allowed. To allow remote management, the allowed ports list should include 8088, 17339, 17336, and ACEmanager port 9191 (or the port you selected for ACEmanager).*

Port Filtering — Outbound

Port Filtering—Outbound restricts LAN access to the external network, i.e., the Internet.

Port Filtering can be enabled to block ports specified or allow specified ports. When enabled, all ports not matching the rule will be allowed or blocked depending on the mode.

Port Filtering can be configured on individual ports or for a range of ports. Click Add More for each port filtering rule you want to add.

Note: Outbound restrictions do not apply to responses to inbound data requests. To restrict inbound access, you need to set the applicable inbound filter.

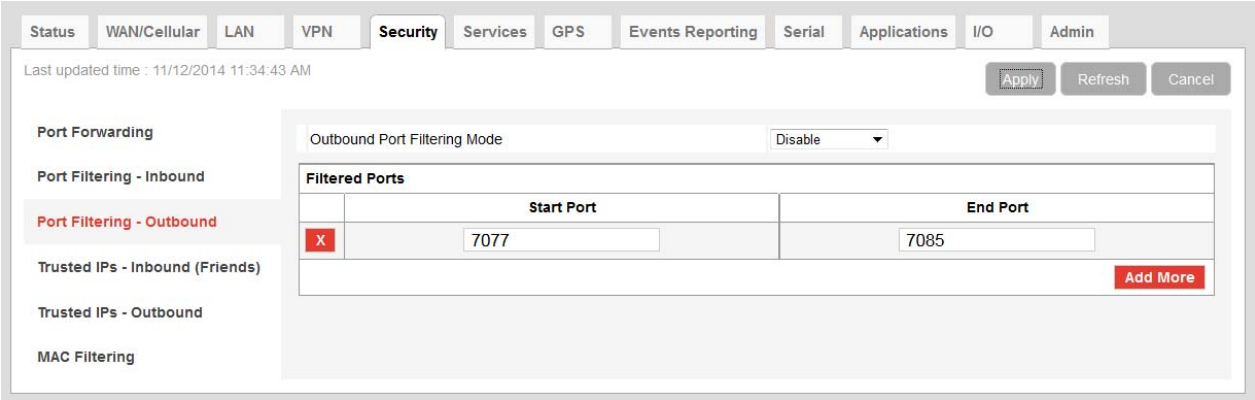


Figure 7-7: ACEmanager: Security > Port Filtering - Outbound

Field	Description
Outbound Port Filtering Mode	Allowed and blocked ports through which traffic is either allowed or blocked (respectively) are listed. Options are: • Disable (default) • Blocked Ports—ports though which traffic is blocked (Shown in Filtered Port s list) • Allowed Ports—ports through which traffic is allowed (Shown in Filtered Port s list) *Note: Outbound IP filter supports up to 9 ports.*
Start Port	The first of a range or a single port on the LAN
End Port	The end of the range on the LAN

Trusted IPs—Inbound (Friends)

Trusted IPs—Inbound restricts unsolicited access to the AirLink device and all LAN connected devices.

Tip: *Trusted IPs-Inbound was called Friends List in legacy AirLink products.*

When enabled, only packets with source IP addresses matching those in the list or range of trusted hosts will have unrestricted access to the AirLink device and/or LAN connected devices.

Note: Inbound restrictions do not apply to responses to outbound data requests. To restrict outbound access, you need to set the applicable outbound filter.

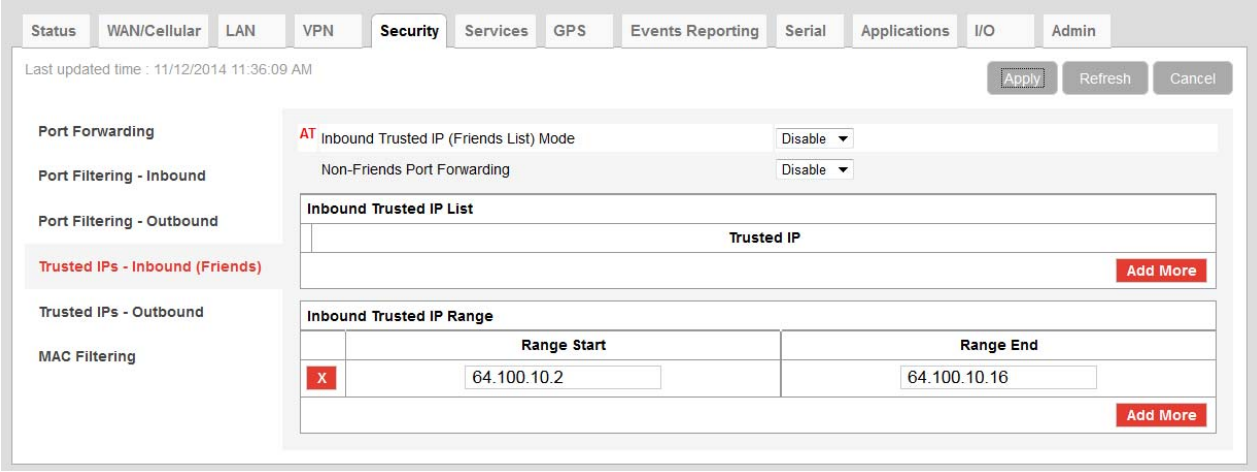


Figure 7-8: ACEmanager: Security > Trusted IPs > Inbound (Friends)

Field	Description
Inbound Trusted IP (Friends List) Mode	Disables or Enables port forwarding rules. Options are Disable (default) or Enable.
Non-Friends Port Forwarding	Non-Friends port forwarding is like an allow rule for any of the forwarded ports. If it is enabled, the port forwarding rules apply to all incoming packets. If it is disabled, only Inbound Trusted List (or Range) IPs get through. Options are Disable (default) or Enable.
Inbound Trusted IP List	Enter a single trusted IP address for example 64.100.100.2. Click Add More to add additional IP addresses to the list.
Inbound Trusted IP Range	Use this section of the page to enter a range of trusted IP addresses.
Range Start	Specify the start and end IP addresses for the trusted IP address range, for example, entering 64.100.10.2 as the Range Start and 64.100.10.15 as the Ranges End would allow 64.100.10.5 but would not allow 64.100.10.16.
Range End	

Trusted IPs—Outbound

Trusted IPs—Outbound restricts LAN access to the external network (Internet).

When enabled, only packets with the destination IP addresses matching those in the list of trusted hosts will be routed from the LAN to the external location.

Note: Outbound restrictions do not apply to responses to inbound data requests. To restrict inbound access, you need to set the applicable inbound filter.

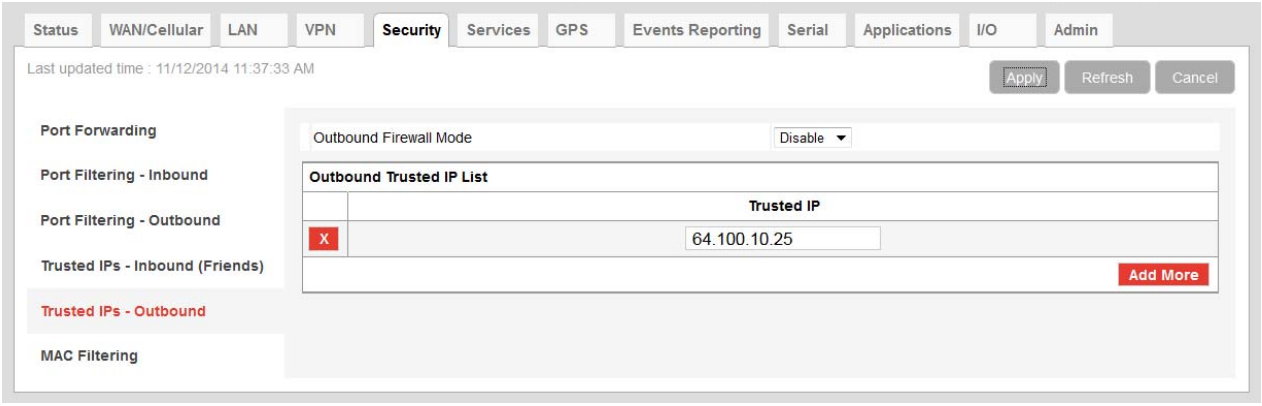


Figure 7-9: ACEmanager: Security > Trusted IPs - Outbound

Field	Description
Outbound Firewall Mode	Disables or enables the Outbound Firewall Options are: • Disable (default)—Allows all outbound traffic • Enable—Only outbound traffic destined for an IP address on the Trusted IP list is allowed. All other outbound traffic is blocked.
Outbound Trusted IP List	Each entry can be configured to allow a single IP address (e.g., 64.100.100.2) Click Add More to add additional IP addresses to the list.

MAC Filtering

MAC filtering restricts LAN connection access. You can create a list of up to 20 devices that are allowed a connection based on their MAC address. When MAC filtering is enabled, devices not on the allowed list are explicitly blocked. Hosts directly connected to the device but not in the Allowed list may show an active physical connection, but are blocked from sending traffic of any kind to the device or any other host connected to the device.

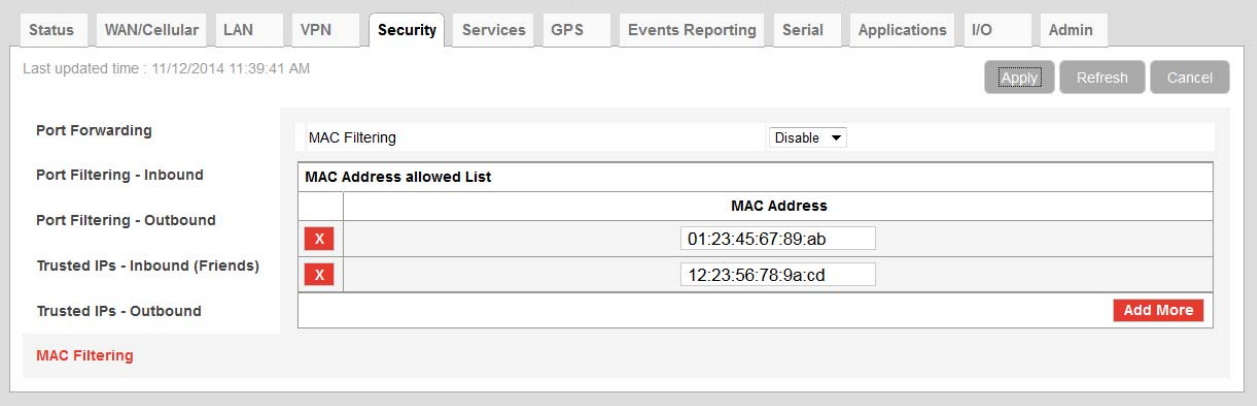


Figure 7-10: ACEmanager: Security > MAC Filtering

Field	Description
MAC Filtering	Enable or disable (default) MAC Filtering
MAC Address allowed List	Allows devices with the MAC Addresses listed to connect to the host and transfer data. Add MAC addresses by clicking on the Add More button. When adding MAC addresses, use a colon between the digit groups, for example 01:23:45:67:89:ab. *Note: After adding all the desired MAC addresses, reboot the device. The MAC Address allowed List takes effect after the device is rebooted.*
MAC Address	This is the MAC Address of the interface adapter on a computer or other device. **Tip:** *You can use the Status > LAN/Wi-Fi page to obtain the MAC addresses of DHCP connected hosts.*

8: Services Configuration

The Services tab sections allow the configuration of external services that extend the functionality of the AirLink Device.

AVMS (AirVantage Management Service)

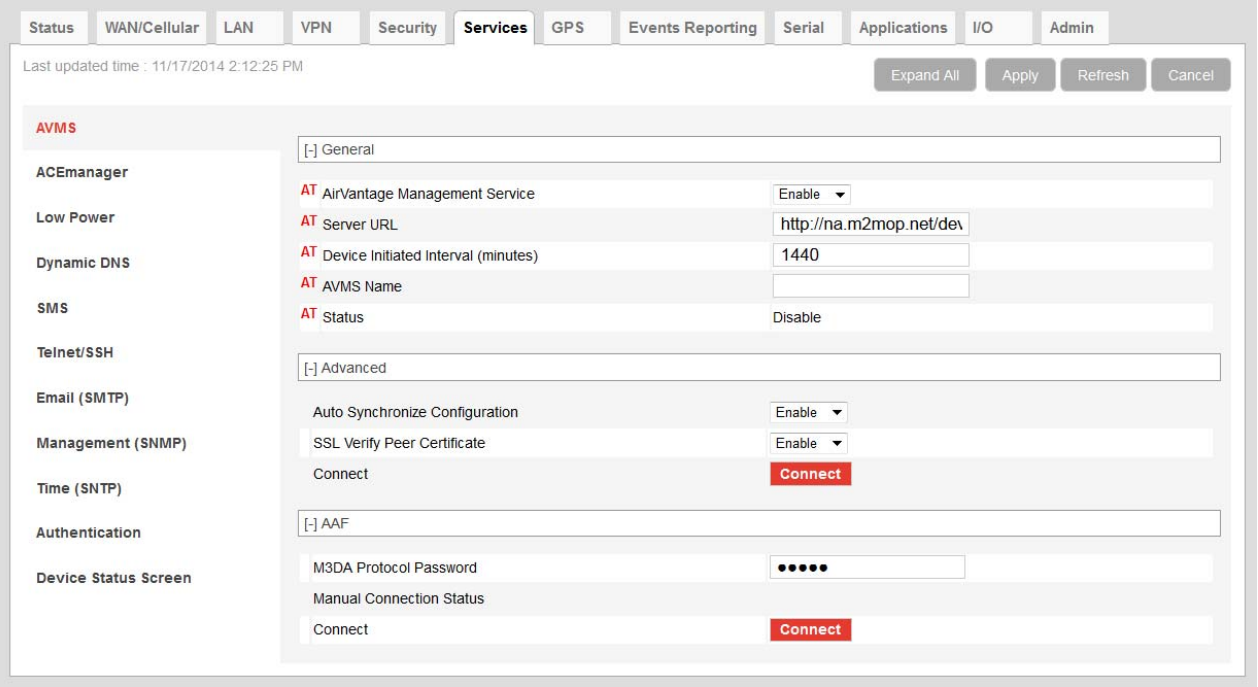


Figure 8-1: ACEmanager: Services > AVMS

Field	Description
General	
AirVantage Management Service	Disables or enables AVMS management by disabling or enabling periodic device-initiated communication with the AVMS server.

Field	Description
Server URL	The AVMS server URL address. By default, this is: http://na.m2mop.net/device/msci/com If you want network traffic from ALEOS to AVMS to be encrypted, enter an HTTPS URL (for example, https://na.m2mop.net/device/msci/com) in this field. Using an HTTPS URL enables Secure Socket Layer (SSL). If SSL is enabled and the SSL Verify Peer Certificate field is set to Enable, the validity of the server certificate is checked. For more information, see SSL Verify Peer Certificate on page 183. *Note: The URL from earlier ALEOS versions, http://na.m2mop.net/device/msci, is still valid. If your AirLink devices are using that URL, there is not need to update it.*
Device Initiated Interval (minutes)	This field determines how often the AirLink device checks for software updates and settings changes from AVMS. AVMS can also query the AirLink device at a regular interval if settings allow. Refer to AirVantage Management Service documentation for more information. Default: 1440 minutes (24 hours).
AVMS Name	Use this field to assign a name of your choice to the AirLink device.This name is used by the AVMS server to identify your device. By default, this field is blank. You can also use an AT command to assign or query the name. See *AVMS_NAME on page 413.
Status	Displays the status of the AVMS connection: • Success—Device successfully contacted AVMS during its latest communication. • Disable—AVMS communications are disabled. (Appears when the AirVantage Management Service drop-down menu is set to Disable.) • [ALEOS] Waiting for connectivity— This transitory status appears when the device is in Connect-on-traffic mode and is trying to connect to the network for an AVMS check-in. (See Always on connection on page 82.) When the device connects to the network, the AVMS check-in is sent and the status changes to Success or an error message, if there is a problem with the connection. For a list of error messages, see page 462.
Advanced	
Auto Synchronize Configuration	This field allows you to choose when changes to the configuration are propagated to AVMS. • Enable—Changes to the configuration are propagated as soon as possible and do not wait for the next communication period (as configured in the Device Initiated Interval field). This may result in more frequent communication with AVMS. (default) • Disable—Changes to the configuration are propagated to AVMS at the device initiated interval rate.

Field	Description
SSL Verify Peer Certificate	This field has no effect unless an HTTPS URL is used for the Server URL. Using an HTTPS URL (for example, https://na.m2mop.net/device/msci/com) as the server URL enables Secure Socket Layer (SSL). When SSL is enabled, use this field to set the SSL certificate validation. • Enable—The validity of the server certificate is checked during the SSL negotiation. (default) If the certificate is not valid, communication with the AVMS server is terminated. For more information, see [HTTP] SSL peer certificate or SSH remote key was not OK on page 463. • Disable—The validity of the server certificate is not checked during the SSL negotiation. The SSL communication proceeds even if the server presents a non-validated certificate.
Connect	The Connect button enables you to manually connect an AirLink device to AVMS. This may be useful for troubleshooting the connection between the platform and the remote device and confirming that AAF scripts or jobs created are executing as expected on AVMS.
AAF	
M3DA Protocol Password	M3DA Protocol Password This password must be configured on the AirLink device and on AVMS. The default password is 12345.
Manual Connection Status	Displays the current manual connection status.
Connect	The Connect button enables you to manually connect an AirLink device to AVMS. This may be useful for troubleshooting the connection between the platform and the remote device and confirming that AAF scripts or jobs created are executing as expected on AVMS.

ACEmanager

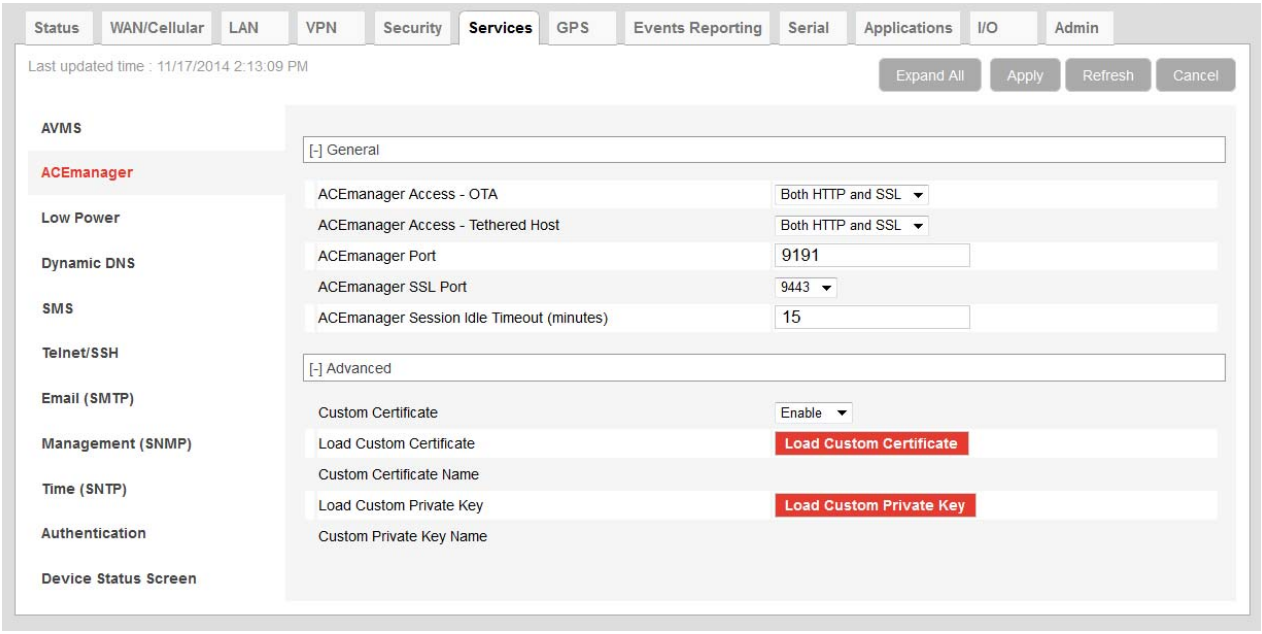


Figure 8-2: ACEmanager: Services > ACEmanager

Field	Description
General	
ACEmanager Access - OTA	Configures over-the-air ACEmanager access. Options are: • OFF • SSL Only • Both HTTP and SSL (default)
ACEmanager Access - Tethered Host	Configures ACEmanager access if tethered (physically connected) to Ethernet, USB, or RS232. Options are: SSL Only and Both HTTP and SSL. (default)
ACEmanager Access - Wi-Fi	Configures ACEmanager access if connected to a Wi-Fi network. Applies only to GX Series devices.
ACEmanager Port	Identifies the port set for ACEmanager. Reboot the device after applying the port change.
ACEmanager SSL Port	Identifies the SSL port set for ACEmanager access. Reboot the device after applying the port change. Options are: • 9443 through 9449 and 443. Default: 9443
ACEmanager Session Idle Timeout (minutes)	If ACEmanager is idle for the configured timeout, it automatically logs out and returns you to the login screen. Options are: • 0–60 (minutes) Default is 15. If you set the ACEmanager Session Idle Timeout to zero (0), the session remains active until you manually log out.

Field	Description
Advanced	
Custom Certificate	Enabling this feature allows you to load a custom SSL certificate. (Some restrictions apply; see Note below for details.) Options are: • Enable—Additional fields appear that allow you to load a custom SSL certificate and a custom private key. The ACEmanager web server uses this custom certificate for authentication during HTTPS communication, instead of the default certificate. • Disable—The ACEmanager web server uses the default SSL certificate for authentication during HTTPS communication. (default) *Note: The custom certificate and private key must meet the following conditions:* • *The certificate must be an X.509 certificate* • *The certificate and the private key must be in .pem format, and they must be in separate files.* • *The encryption cipher suite used must be 128 bits.* • *There is no limit to the size of the private key, but the larger the key, the more the performance is affected. Sierra Wireless recommends that the key does not exceed 2048 bits.*
Load Custom Certificate	This field only appears when the Custom Certificate field is set to Enable. To load a custom SSL certificate: 1. Click Load Custom Certificate. 2. Click Browse... and navigate to the SSL certificate file. 3. Click Upload file to device. 4. Once you have uploaded the custom certificate and the custom private key, click Apply and reboot the device.
Custom Certificate Name	This field only appears when the Custom Certificate field is set to Enable. Displays the name of the custom certificate.
Load Custom Private Key	This field only appears when the Custom Certificate field is set to Enable. Allows you to enter a custom private key (Some restrictions apply; see Custom Certificate on page 185 for details.) To load a custom private key: 1. Click Load Private Key. 2. Click Browse... and navigate to the private key file. 3. Click Upload file to device. 4. Once you have uploaded the custom certificate and the custom private key, click Apply and reboot the device.
Custom Private Key Name	This field only appears when the Custom Certificate field is set to Enable. Displays the name of the private key.

Low Power

The AirLink device switches into Low Power Mode when the ACEmanager-configured event occurs.

Low Power Mode is a standby mode whereby the AirLink processor and radio are off and a low power timer and detection circuit are operational. When ACEmanager-configured events are detected, the AirLink device powers up and automatically connects to the Mobile Network Operator's network.

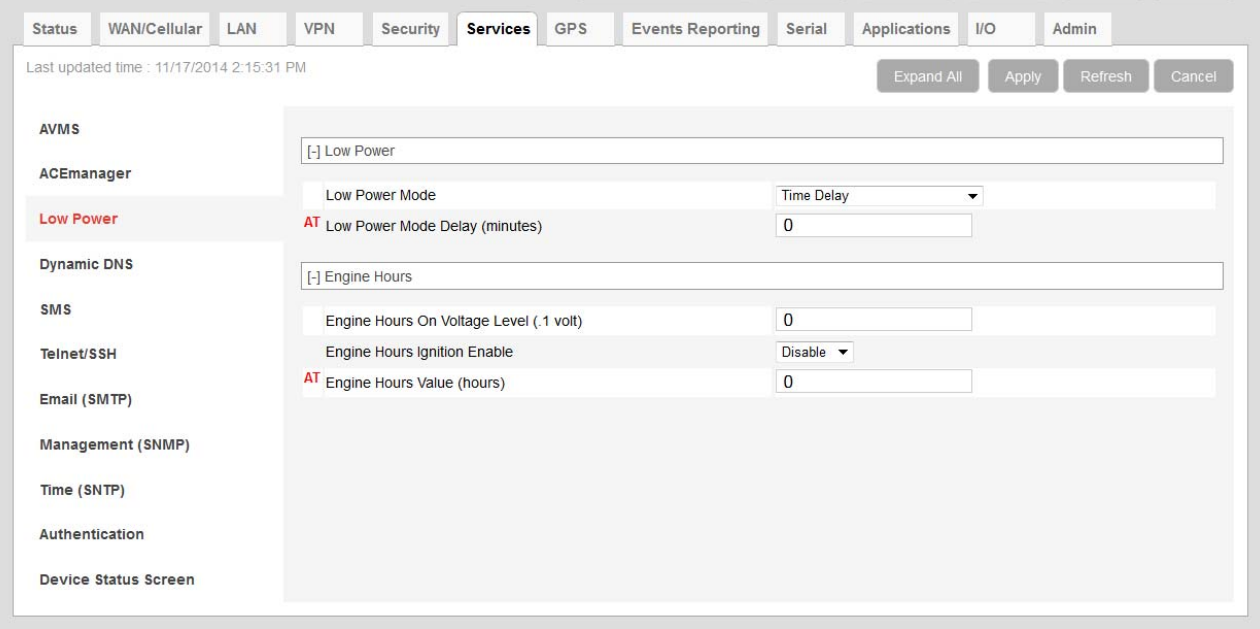
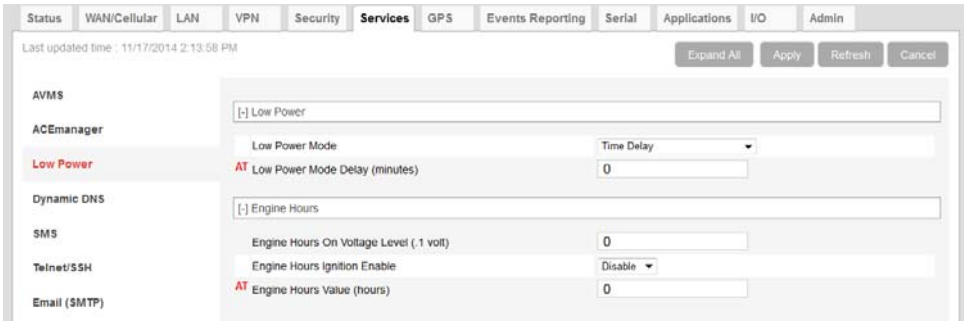
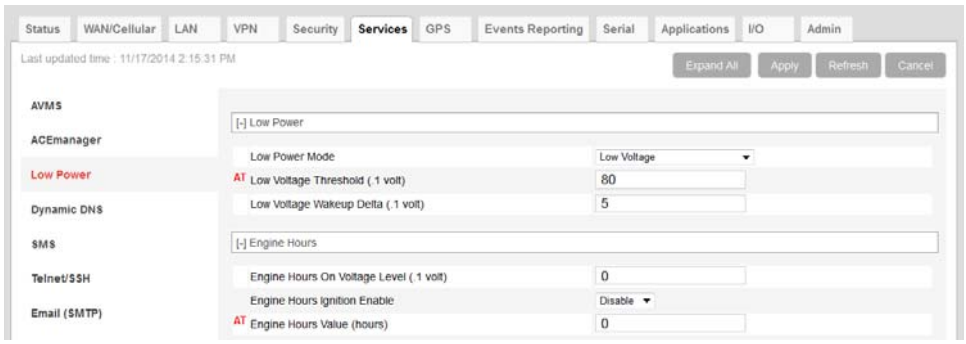
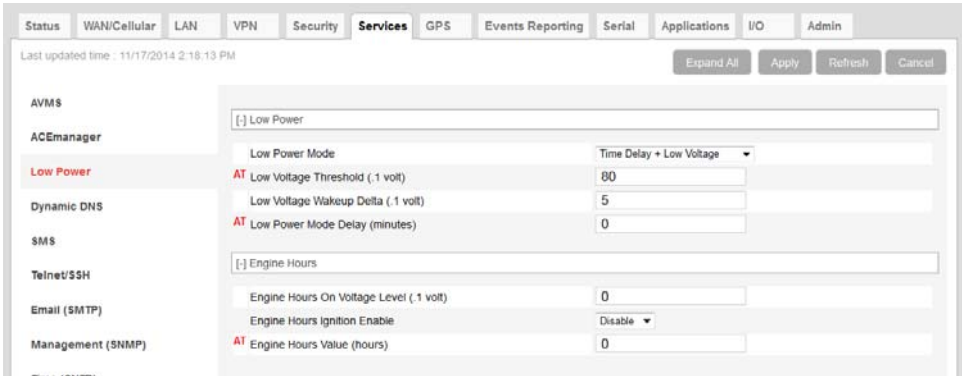
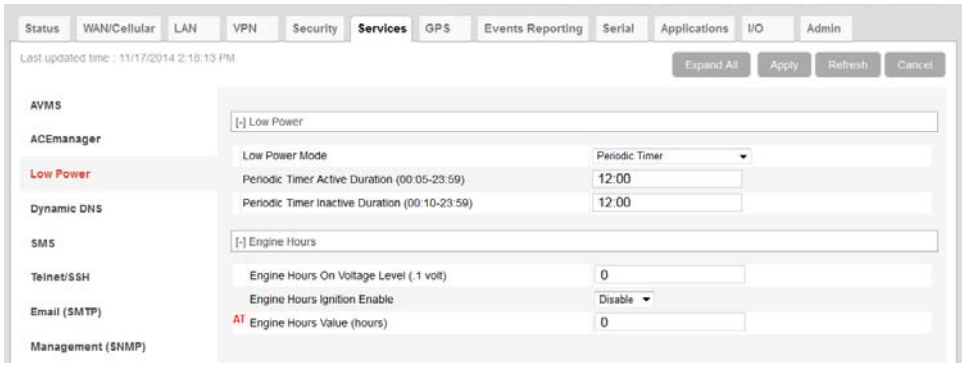
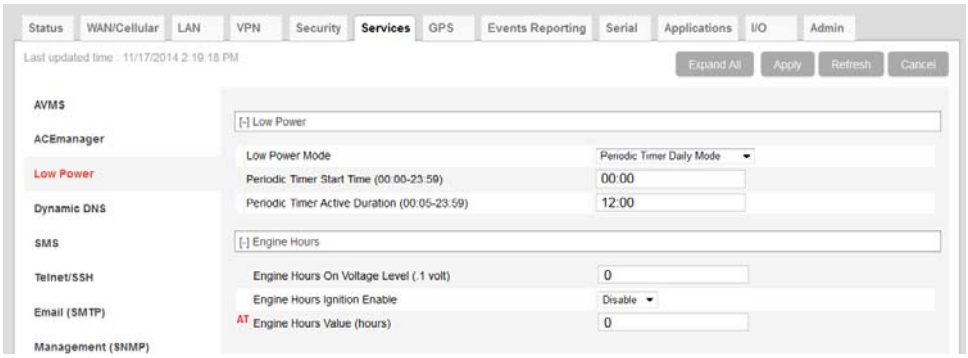


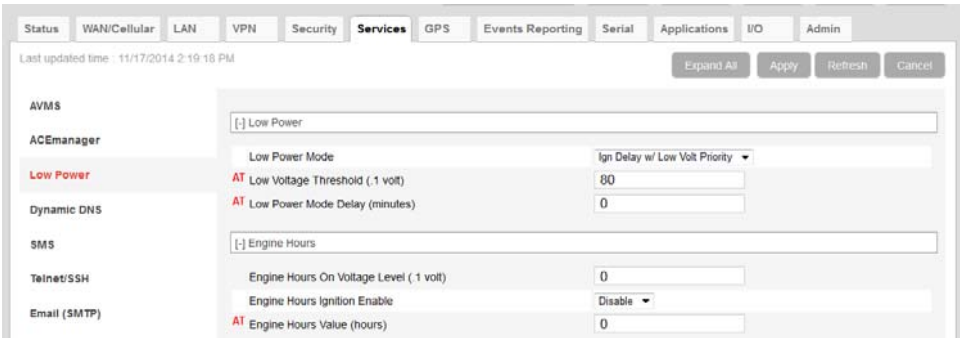
Figure 8-3: ACEmanager: Services > Low Power

Field	Description
Low Power	
Low Power Mode	Allows you to set one of the following low power mode parameters: • Disable (default) • Time Delay • Low Voltage • Time Delay + Low voltage • Periodic Timer • Periodic Timer Daily Mode • Ign Delay w/Low Volt Priority

Field	Description
Low Power Mode (continued)	Time Delay If you select Time Delay, the AirLink device monitors the ignition sense on the power connector and enters the low power consumption stand-by mode when the ignition is turned-off.  • Low Power Mode Delay (minutes): The number of minutes after one of the Low Power events happens until the AirLink device enters the low power mode. (Accepted values 0–255)
Low Power Mode (continued)	Low Voltage If you select Low Voltage, you need to set the Low Voltage Threshold and Low Voltage Wake-up Delta. • Low Voltage Threshold: Set the voltage level at which the device goes into low power mode (threshold in tenths of volts), e.g. VLTG=130 would place the device in a low power standby state if the voltage on the power connector Pin 3 (Ignition Sense) goes below 13.0V. For more information on the power connector pins, refer to the Hardware Configuration User Guide for your AirLink device. Accepted values are 80–360. • Low Voltage Wakeup Delta (.1 volt): Sets the change in voltage used to wake up the device from low power mode, e.g. set to 25 to wake up from low power mode when the input voltage exceeds the low voltage threshold by 2.5 volts. 

Field	Description
Low Power Mode (continued)	Time Delay + Low Voltage If you select this option, the device delays going into Low Power mode when the voltage on the power connector Pin 3 (Ignition Sense) goes below the configured threshold. For more information on the power connector pins, refer to the Hardware Configuration User Guide for your AirLink device.  *Note: There is always a minimum of 1 minute between the power down event and actual shutdown (to give the AirLink device time to prepare); entering zero, for Low Power Mode Delay, will not power down the device immediately.* Accepted values for the Low Power Mode Delay (minutes) field are 0–255
Low Power Mode (continued)	Periodic Timer If you select the Periodic Timer, two additional fields appear: • Periodic Timer Active Duration (00:05–23:59) — Enter the time for how long the device needs to be in Active mode. (Minimum accepted value is 00:05; maximum accepted value is 23:59) Default is 12:00. • Period Timer Inactive Duration (00:10–23:59) — Enter the time for how long the device should be inactive after the Active mode expires. (Minimum accepted value is 00:10; maximum accepted value is 23:59) Default is 12:00. The Low Power mode process will repeat in a cyclical way (active and inactive). 

Field	Description
Low Power Mode (continued)	Periodic Timer Daily Mode This mode allows you to specify when the device should be active and when it should be in Low Power mode on a daily basis. If you select the Periodic Timer Daily Mode, two additional fields display: • Periodic Timer Start Time (00:00–23:59 UTC) — Enter the time to start the AirLink device in the Active mode. (Minimum accepted value is 00:00; maximum accepted value is 23:59) Default is 00:00. • Period Timer Active Duration (00:05–23:59 UTC) — Enter the time for how long the device should be active. (Minimum accepted value is 00:05; maximum accepted value is 23:59) Default is 12:00. The device will become active at the start time (UTC) and stay active for the active duration. 

Field	Description
Low Power Mode (continued)	Ign Delay w/ Low Volt Priority This mode powers down the AirLink device if the vehicle battery, as monitored by power connector Pin 1 (Power pin), drops below a configured value. For more information on the power connector pins, refer to the Hardware Configuration User Guide for your AirLink device. When this mode is selected: • ALEOS monitors the ignition and if the ignition is turned off, the AirLink device goes into low power mode after the configured time. However, if the battery voltage falls below the configured value before the timer expires, the device goes into low power mode 10 seconds later. • If the ignition is on and the voltage falls below the configured value for more than 10 seconds, the device goes into low power mode. If you select the Ign Delay w/ Low Volt Priority Mode, two additional fields appear: • Low Voltage Threshold (.1 volts): Set the voltage level below which the device goes into low power mode. • Low Power Mode Delay (minutes): Set the time delay between the ignition being turned off and the AirLink device going into low power mode. (Accepted values are 0–255) 
Engine Hours—ALEOS can start and stop counting engine hours based on: • Voltage on power connector Pin 1 (Power pin) from the vehicle battery (Engine Hours On Voltage Level) • Voltage on power connector Pin 3 (Ignition Sense pin) (Engine Hours Ignition Enable) If you configure both fields, both conditions must be met before the device begins counting engine hours. For more information on the power connector pins, refer to the Hardware Configuration User Guide for your AirLink device. 	
Engine Hours On Voltage Level (.1 Volt)	If you want to use this field to trigger counting engine hours, the AirLink device must be using the vehicle battery as a power source (i.e. Pin 1 [VCC] and Pin 2 [ground] on the AirLink device's power connector are connected to the vehicle battery). Enter the voltage level above which the AirLink device starts counting engine hours. When the voltage from the vehicle battery falls below that value, the device stops counting engine hours. Enter the desired value of the ignition.e in .1 volt units. For example, to set the voltage level at 13.0 volts, enter 130. The default value is 0, which means the feature is disabled. Engine hours are not incremented based on the power pin voltage level.

Field	Description
Engine Hours Ignition Enable	If Pin 3 (the ignition sense pin) on the AirLink device's power connector is wired to the vehicle's ignition switch, oil pressure switch, or some other digital input, you can use this field to trigger counting engine hours. The device starts counting engine hours when the voltage on Pin 3 is high and stops counting when the voltage is low (Ground or 0 volts). For more information on the power connector pins, refer to the Hardware Configuration User Guide for your AirLink device. Options are: • Disable (default) Engine hours are not incremented based on changes to Pin 3. • Enable
Engine Hours Value (hours)	Displays an estimate of the number of hours the engine has been running, based on either the input voltage from the vehicle battery or the voltage on the ignition sense pin, depending on which of the two previous fields you configured. For more information on the power connector pins, refer to the Hardware Configuration User Guide for your AirLink device. You can also set the engine hours value to an initial value. The initial default value is 0. The maximum allowed value is 65535. You can also use an AT Command to set this value. For more information, see *ENGHRS on page 413. *Note: You can configure Events Reporting to send reports based on this value. For more information, see Events Reporting Configuration on page 257.*

Dynamic DNS

Dynamic DNS allows an AirLink device WAN IP address to be published either to a proprietary Sierra Wireless dynamic DNS service called IP Manager, or to an alternate 3rd party Mobile Network Operator.

Whether you have one Sierra Wireless AirLink device or multiple devices, it can be difficult to keep track of the current IP addresses especially if the addresses are not static but change every time the devices connect to the cellular network. If you need to connect to a specific gateway, or the device behind it, it is much easier when you have a domain name (car54.mydomain.com, where are you?).

Reasons to Contact or Connect to a Device:

- Requesting a location update from a delivery truck
- Contacting a surveillance camera to download logs or survey a specific area
- Triggering an oil derrick to begin pumping
- Sending text to be displayed by a road sign
- Updating the songs to be played on a juke box
- Updating advertisements to be displayed in a cab
- Remote accessing a computer, a PLC, an RTU, or other system
- Monitoring and troubleshooting the status of the device itself without needing to bring it in or go out to it.

A dynamic IP address is suitable for many Internet activities such as web browsing, looking up data on another computer system, for data only being sent out, or for data only being received after an initial request (also called Mobile Originated). However, if you need to contact the AirLink device directly, a device connected to the AirLink device, or a host system using your AirLink device (also called Mobile Terminated), a dynamic IP will not give you a reliable address to contact (since it may have changed since the last time it was assigned).

Domain names are often only connected to static IP addresses because of the way most domain name (DNS) servers are set-up. Dynamic DNS servers require notification of IP Address changes so they can update their DNS records and link a dynamic IP address to the correct name.

- Dynamic IP addresses are granted only when your AirLink device is connected and can change each time the gateway reconnects to the network.
- Static IP addresses are granted the same address every time your AirLink device is connected and are not in use when your gateway is not connected.

Since many cellular providers, like wire-based ISPs, do not offer static IP addresses or static address accounts (which can cost a premium as opposed to. dynamic accounts), Sierra Wireless AirLink Solutions developed IP Manager. IP Manager works with a Dynamic DNS server to receive notification from Sierra Wireless AirLink devices to translate the dynamic IP address to a fully qualified domain name. Thus, you can contact your AirLink device directly from the Internet using a domain name.

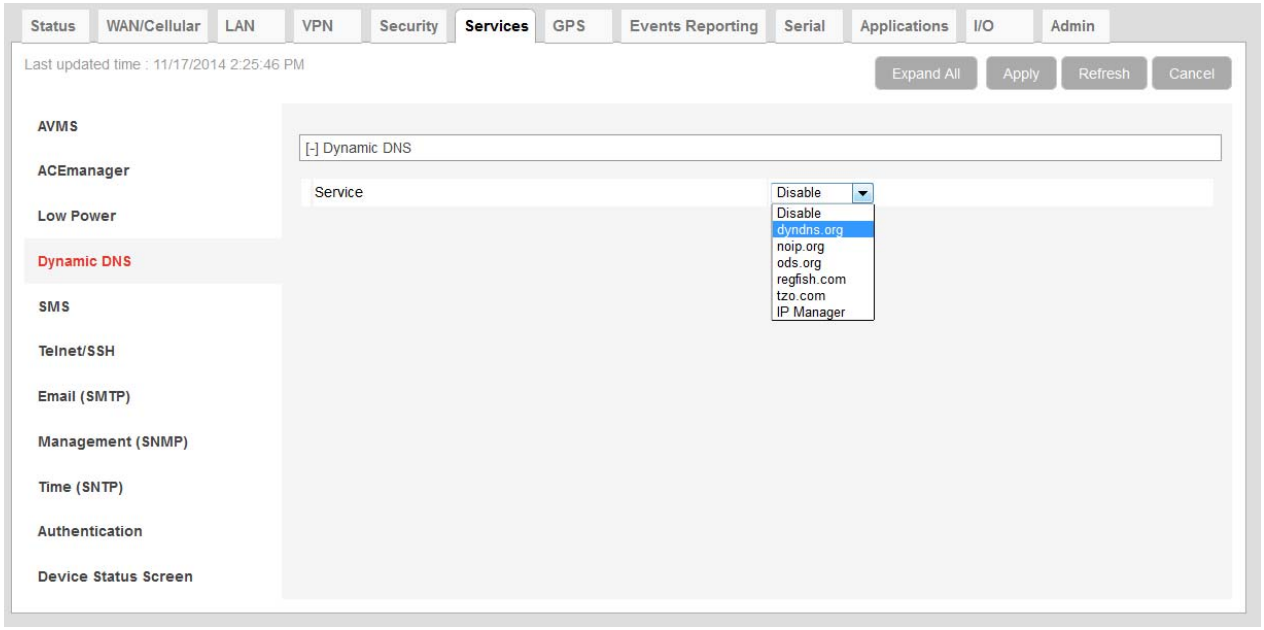


Figure 8-4: ACEmanager: Services > Dynamic DNS Service (partial screen)

Field	Description
Service	Allows you to select a Dynamic DNS Mobile Network Operator. Options are: • Disable (default) • dyndns.org • noip.org • ods.org • regfish.com • tzo.com • IP Manager

3rd party Services

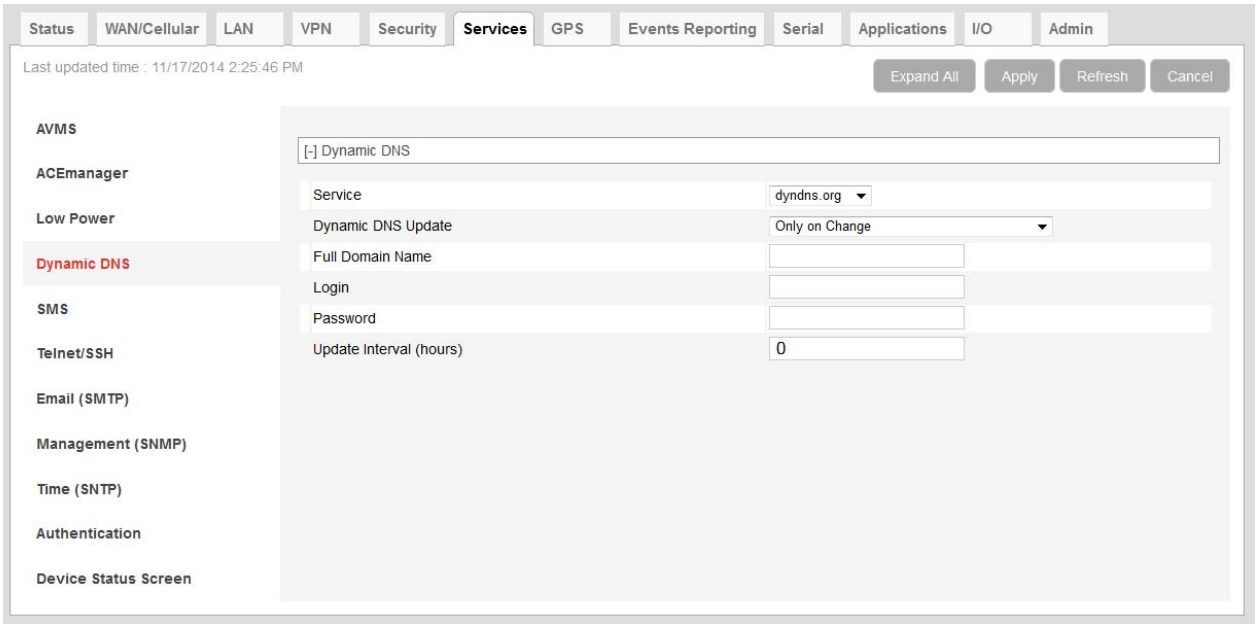


Figure 8-5: ACEmanager: Services > Dynamic DNS 3rd Party Services (partial screen)

Figure 8-5 is a sample 3rd party service information screen. The 3rd party service selected from the Service drop down menu in this example is “dyndns.org.” These same fields will be displayed for all Service selections other than IP Manager and Disable.

Field	Description
Service	Allows you to select a Dynamic DNS Mobile Network Operator. Options are: • Disable (default) • dyndns.org • noip.org • ods.org • regfish.com • tzo.com • IP Manager
Dynamic DNS Update	Options are: • Only on Change • Periodically Update (Not Recommended)
Full Domain Name	The name of a specific AirLink gateway or device
Login	Shows the login name
Password	Shows the password in encrypted format
Update Interval (hours)	Indicates the time (in hours) between checks for service updates from the selected 3rd party service when periodic is selected.

IP Manager

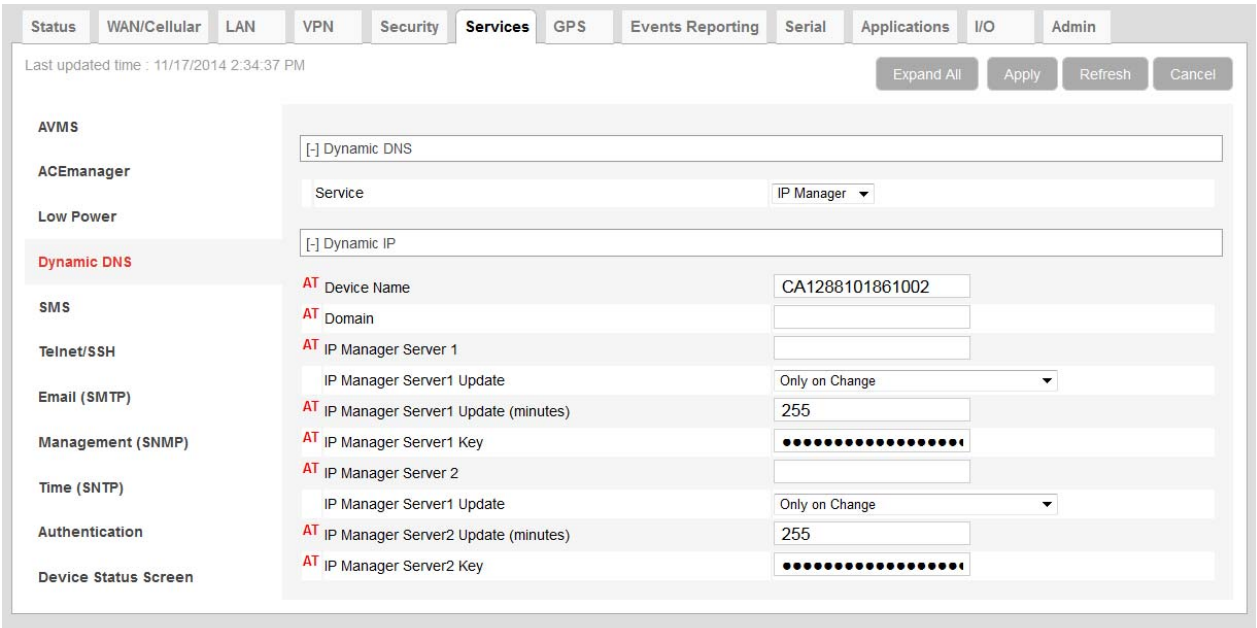


Figure 8-6: ACEmanager: Services > Dynamic DNS IP Manager

Figure 8-6 shows the Dynamic IP fields that appear after selecting IP Manager as your Dynamic DNS Service.

Field	Description
Device Name	The name you want for the device. If you want to use the current device phone number as part of the FQDN (for example, 6175551234.eairlink.com) enter #NETPHONE in this field. #NETPHONE is displayed in this field and everywhere else the device name is used, including on the Home > Status page, in SMS messages, in Event reports, as the PPPoE station name, etc. Using #NETPHONE as the device name is recommended if the account phone number may change and you want the device to continue to use the current phone number as part of the FQDN, or if you are creating a template that will be applied to multiple devices. To use this feature, you must have IP Manager selected in the Service field.
Domain	The domain name to be used by the device. This is the domain name of the server configured for *IPMANAGER1. *Note: As a service, Sierra Wireless maintains IP Manager servers that can be used with any AirLink device. To use one of the free IP Manager servers, enter eairlink.com in this field.*
IP Manager Server 1 (IP Address) / IP Manager Server 2 (IP Address)	The IP address or domain name of the dynamic DNS server which is running IP Manager. *Note: To use the Sierra Wireless IP Manager server, enter:* *edns1.eairlink.com (IP Manager Server 1)* *edns2.eairlink.com (IP Manager Server 2)*
IP Manager Server 1 Update / IP Manager Server 2 Update	Options are: • Only on Change • Periodic
IP Manager Server1 Update (mins) / IP Manager Server2 Update (mins)	How often, in minutes, you want the address sent to the IP Manager
IP Manager Server 1 Key / IP Manager Server 2 Key	User-defined password key used instead of the AirLink secret key when using an IP Manager server other than the one provided by Sierra Wireless.

Tip: *Some PPPoE connections can use a Service Name to differentiate PPPoE devices. Use the device name to set a Station Name for the PPPoE connection.*

Understanding Domain Names

A domain name is a name of a server or device on the Internet associated with an IP address. Similar to how the street address of your house or your phone number are ways to contact you, both the IP address and the domain name can be used to contact a server or device on the Internet. While contacting you at your house address or with your phone number employ different methods, using a domain name instead of the IP address uses the same method, just as a word based name is easier for most people to remember than a string of numbers.

Understanding the parts of a domain name can help to understand how IP Manager works and what you need to be able to configure the device. A fully qualified domain name (FQDN) generally has several parts.

- **Top Level Domain** (TLD): The TLD is the ending suffix for a domain name (.com, .net, .org, etc.)
- **Country Code Top Level Domain** (ccTLD): This suffix is often used after the TLD for most countries except the US (.ca, .uk, .au, etc.)
- **Domain name**: This is the name registered with ICANN (Internet Corporation for Assigned Names and Numbers) or the registry for a the country of the ccTLD (i.e., if a domain is part of the .ca TLD, it would be registered with the Canadian domain registry). A name must be registered before it can be used.
- **Sub-domain or server name**: A domain name can have many sub-domain or server names associated with it. Sub-domains need to be registered with the domain, but do not need to be registered with ICANN or any other registry. It is the responsibility of a domain to keep track of its own subs.

car54.mydomain.com

- ***.com*** is the TLD
- *mydomain* is the domain (usually noted as mydomain.com since the domain is specific to the TLD)
- *car54* is the subdomain or server name associated with the device, computer, or device registered with mydomain.com

car54.mydomain.com.ca

This would be the same as above, but with the addition of the country code. In this example, the country code (.ca) is for Canada.

Tip: *A URL (Universal Resource Locator) is different from a domain name in that it also provides information on the protocol used by a web browser to contact that address such as* `http://www.sierrawireless.com`. www.sierrawireless.com *is a fully qualified domain name, but http://, the protocol identifier, is what makes the whole thing a URL.*

Dynamic Names

When an IP address is not expected to change, the DNS server can indicate to all queries that the address can be cached and not looked up for a long period of time. Dynamic DNS servers, conversely, have a short caching period for the

domain information to prevent other Internet sites or queries from using the old information. Since the IP address of a device with a dynamic account can change frequently, if the old information was used (e.g., with a DNS server which indicates the address can be cached for a long period of time) when the IP address changed, the domain would no longer point to the new and correct IP address of the device.

If your AirLink device is configured for Dynamic IP when it first connects to the Internet, it sends an IP change notification to the IP Manager. The IP Manager acknowledges the change and updates the Dynamic DNS server. The new IP address will then be the address for your device's configured name.

When your device IP address has been updated in IP Manager, it can be contacted by name. If the IP address is needed, use the domain name to determine the IP address.

Note: The fully qualified domain name of your AirLink device will be a subdomain of the domain used by the IP Manager server.

Wi-Fi Landing Page

The Wi-Fi Landing Page allows you to enable or disable the Landing Page identified by a Landing Page URL address.

This page only appears if a Wi-Fi X-Card is installed in the AirLink device.

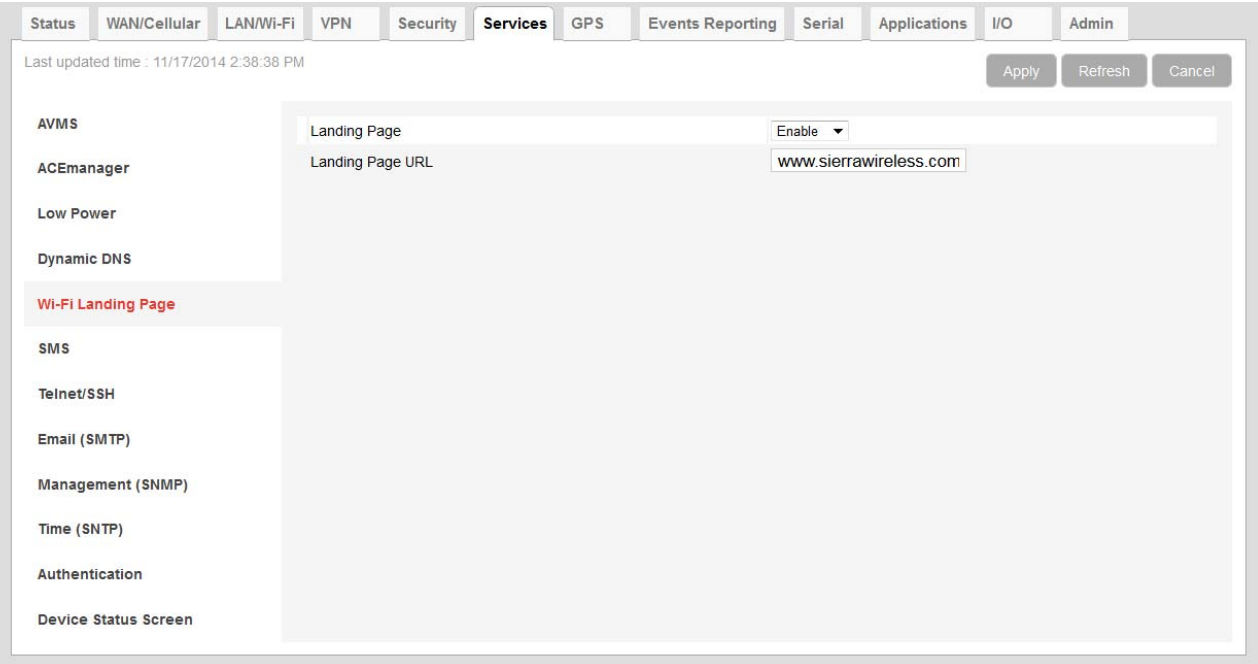


Figure 8-7: ACEmanager: Services > Wi-Fi Landing Page

Field	Description
Landing Page	Allows you to enable or disable (default) the Wi-Fi landing page.
Landing Page URL	A valid URL address is required to enable Internet service. This URL can include folders or subdomains (e.g., www.sierrawireless.com/airlink)

SMS Overview

AirLink devices can:

- Receive commands via SMS message and send responses, even when the device does not have a data connection (for example, you can provision a device via SMS without having a data connection)
- Act as an SMS gateway for a device connected to a local interface

Note: To use SMS with your AirLink device, you must have an account with SMS enabled.

ACEmanager has four SMS modes. Table 8-1 summarizes the capabilities of each mode.

Table 8-1: SMS Mode Capabilities

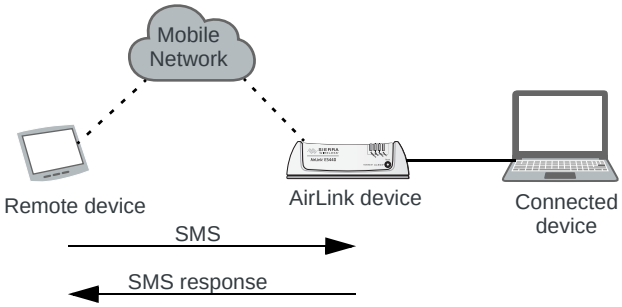
Mode	SMS Command with password	SMS Command without password	SMS Gateway
Password Only	Yes	No	No
Control Only	Yes	Yes*	No
Gateway Only	Yes	No	Yes*
Control & Gateway	Yes	Yes*	Yes*

* Provided either:

- Trusted Phone Number List is disabled.
- Trusted Phone Number List is enabled and the device's phone number is in the Trusted Phone Number List.

For more information on Trusted Phone Number List, see Inbound SMS Messages on page 211.

Sending SMS Commands to an AirLink Device



The format for sending an SMS command varies depending on the mode. See Table 8-2 for details.

Table 8-2: SMS Command Formats

Mode	SMS Command Format
Password Only	PW [Password] [Prefix][Command]
Control Only (from a number on the Trusted Phone Number list)	[Prefix][Command] or PW [Password] [Prefix][Command]
Control Only (from a number not on the Trusted Phone Number list)	PW [Password] [Prefix][Command]
Gateway Only	PW [Password] [Prefix][Command]

Note: Insert a space before and after [Password]; no space between [Prefix] and [Command].

Examples:

[Prefix][Command]

“&&&reset”, where:

- &&& is the prefix
  If the ALEOS Command Prefix field in ACEmanager (Services > SMS) is blank, the prefix is not required.
- reset is the command

PW [Password] [Prefix][Command]

“PW 1234 &&&reset”, where:

- 1234 is the password
  For more information, see SMS Password Security on page 213.
- &&& is the prefix
  If the ALEOS Command Prefix field in ACEmanager (Services > SMS) is blank, the prefix is not required.
- reset is the command

For information on sending SMS commands and a list of available commands, see page 447.

SMS Modes

The following sections provide instructions for configuring each of these modes and sending SMS messages:

- Password Only
- Control Only
- Gateway Only
- Control and Gateway

For a list of available SMS commands, see page 447. For a list of SMS-related AT commands, see SMS on page 416.

Password Only

In Password Only mode, you can send SMS commands to a device, provided you use the password. Gateway SMS messaging is not supported in this mode.

Note: In Password Only mode, the password is always required. The Trusted Phone Number List is not available.

To configure Password Only mode:

1. In ACEmanager, go to Services > SMS.

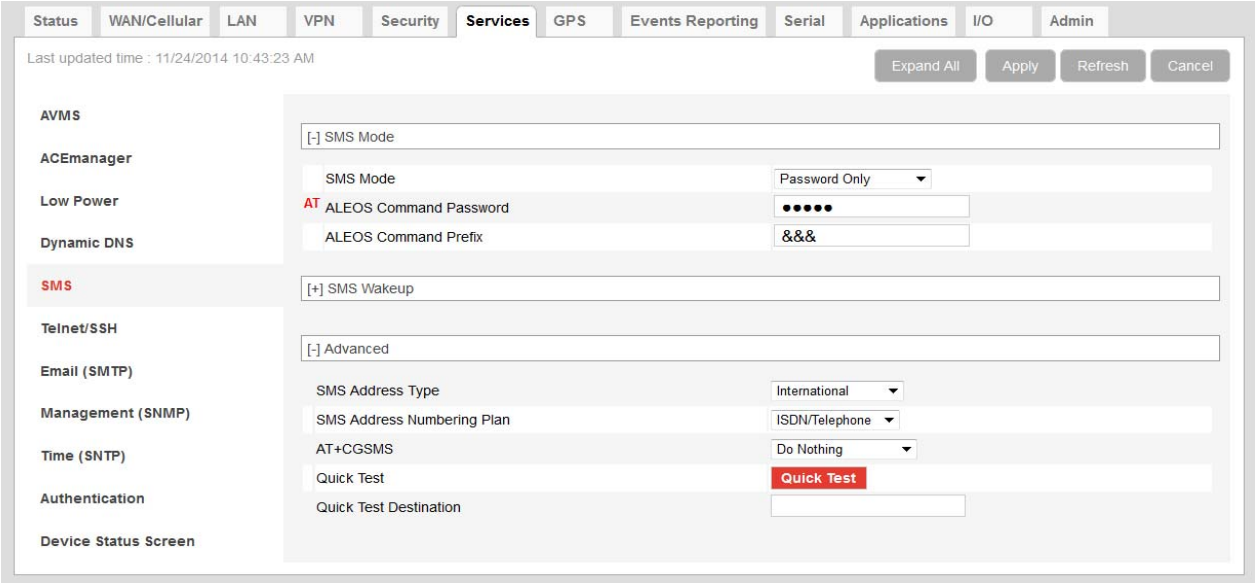


Figure 8-8: ACEmanager: Services > SMS (Password Only)

2. In the SMS Mode field, select Password Only.
3. Enter the desired password in the ALEOS Command Password field or leave the field blank to use the default password.

   The password you enter can be any alphanumeric string between 1 and 255 characters long.

   For more information see SMS Password Security on page 213.

4. If desired, configure SMS Wakeup (see SMS Wakeup on page 210) and Advanced options (see SMS > Advanced on page 214).
5. Click Apply.

For information on the message format, see Sending SMS Commands to an AirLink Device on page 199.

Control Only

In Control Only mode, you can send SMS commands to an AirLink device, but you cannot send non-command (gateway) SMS messages.

You can send an SMS command without a password if:

- Trusted Phone Number is disabled.
- Trusted Phone Number is enabled and your phone number is on the Trusted Phone Number List.

If Trusted Phone Number is enabled and your number is not on the Trusted Phone Number List, you can still send an SMS command provided you use the password.

Configure ALEOS for Control Only mode

1. In ACEmanager, go to Services > SMS.

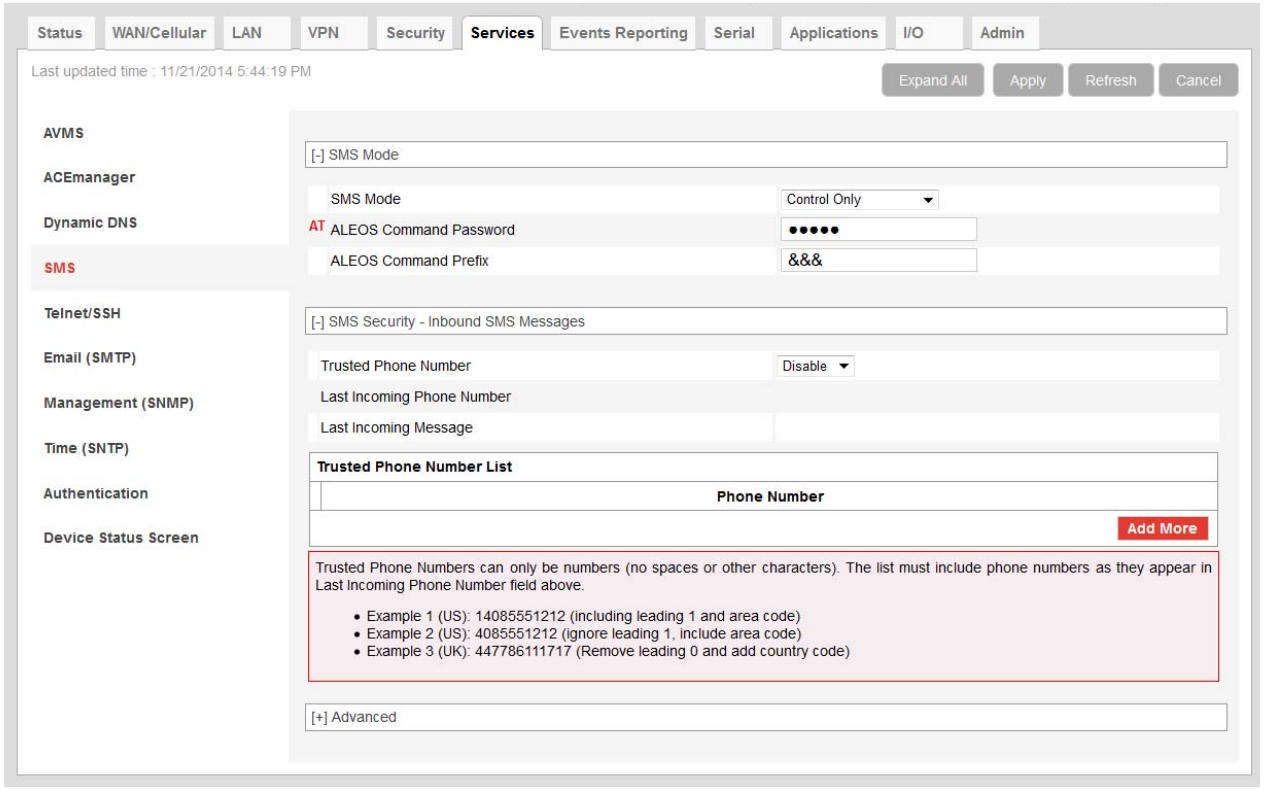


Figure 8-9: ACEmanager: Services > SMS (Control only)

2. In the SMS Mode field, select Control Only.

3. Enter the desired password in the ALEOS Command Password field or leave the field as is to use the default password.

   The password you enter can be any alphanumeric string between 1 and 255 characters long.

   For more information see SMS Password Security on page 213.

Note: If all the SMS commands you send in Control Only mode are from a trusted number, you do not need to include a password when you send the command.

4. If desired, change the ALEOS Command Prefix or use the default prefix, &&&.

Note: If you leave the ALEOS Command Prefix field blank, no prefix is required when you send the SMS command. The option to omit the prefix is only available in Control Only mode.

5. If desired, configure SMS Security options (see SMS Security on page 211), SMS Wakeup (see SMS Wakeup on page 210), and Advanced options (see SMS > Advanced on page 214).
6. Click Apply.

For information on the message format, see Sending SMS Commands to an AirLink Device on page 199.

Gateway Only

In Gateway Only mode you can send and receive SMS gateway messages through the AirLink device to a local device. SMS messages received by the AirLink device (inbound) are sent on to the configured local device. Messages sent by the local device to a configured port on the AirLink device are sent out as SMSs (outbound) to a remote destination. Essentially, the AirLink device sends SMS messages between the cellular radio and the connected device.

In Gateway Only mode, you can also send SMS commands provided you include a password. For more information, see Sending SMS Commands to an AirLink Device on page 199.

To configure ALEOS for Gateway Only mode and format a Gateway message:

1. In ACEmanager, go to Services > SMS.

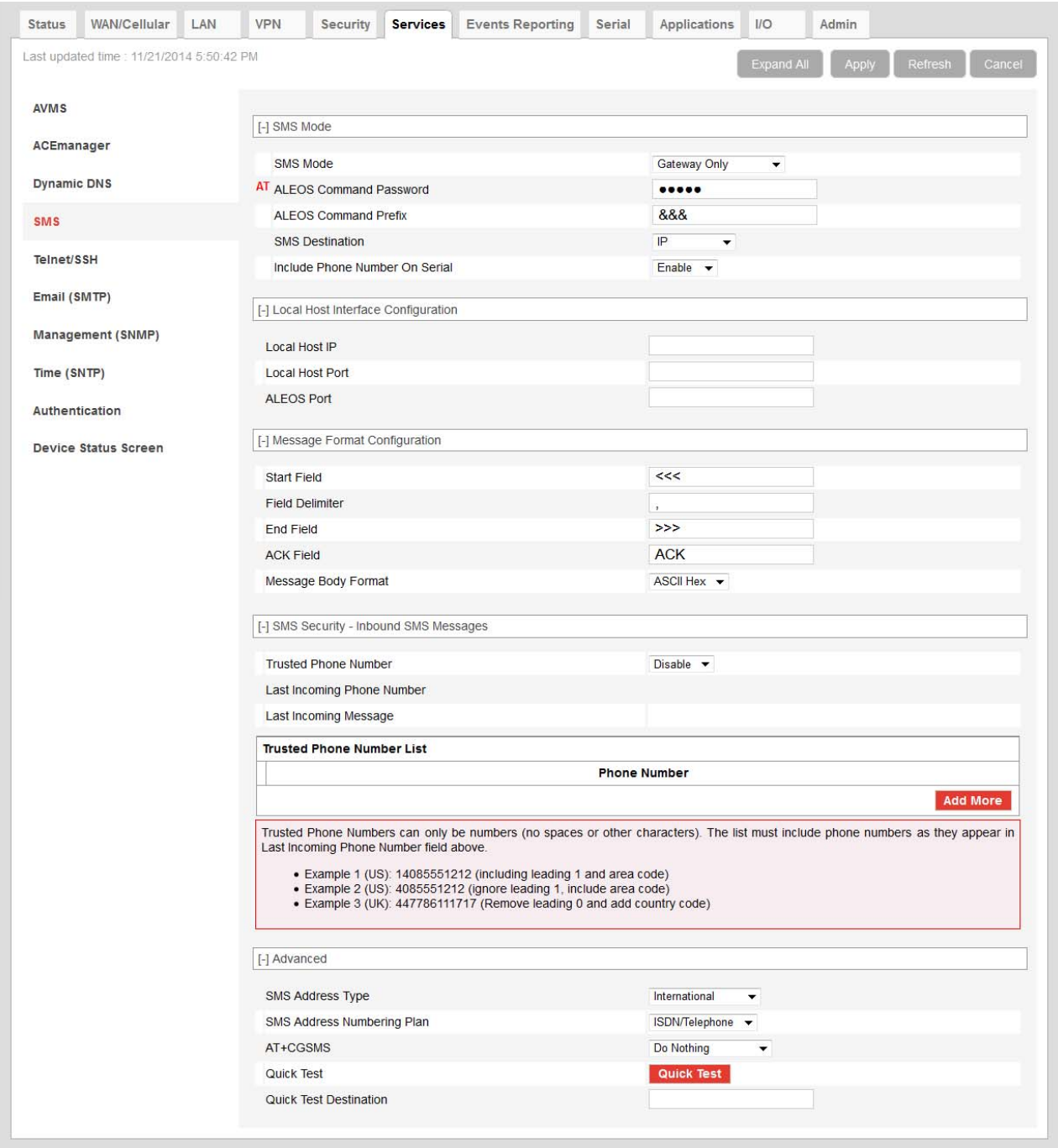


Figure 8-10: ACEmanager: Services > SMS (Gateway Only)

2. In the SMS Mode field, select Gateway Only.
3. Enter the desired password in the ALEOS Command Password field or leave the field blank to use the default password.

   The password you configure can be any alphanumeric string between 1 and 255 characters long.

   For more information see SMS Password Security on page 213.

4. The SMS destination is the local interface where ALEOS forwards an SMS from the mobile network.
   In the SMS destination field, select from the following options:
   - Serial—Messages are forwarded to the Serial port on the destination device.

     If you want to include the phone number as part of the information sent to the serial port, select Yes in the Include Phone Number on Serial field.

     Proceed to step 13.
   - IP—Messages are sent using UDP over IP to a designated LAN or Wi-Fi device. Proceed to step 5.

Local Device Interface Configuration (Applies to inbound [to the local device] gateway messages when IP is the SMS destination and outbound [from the local device])

Inbound

5. Enter the Local Host IP address.

   This is the IP address of the LAN or Wi-Fi device that is used as the destination for all incoming Gateway messages.
6. Enter the Local Host Port.

   This is the UDP port the destination device listens to for incoming messages.

Outbound

7. Enter the ALEOS port.

   This is the UDP port on which the AirLink device listens for outbound Gateway messages sent from any local device.

Message Format Configuration (Only applies if you selected IP in the SMS destination field)

8. In the Start field, enter the start of message delimiter, or use the default (<<<).
9. In the Field Delimiter field, enter the delimiter to be used between fields in the SMS message, or use the default (,).
10. In the End field, enter the end of message delimiter, or use the default (>>>).
11. In the ACK field, enter the desired acknowledgment message, or use the default (ACK). The acknowledgment is sent to the device as a UDP packet on the same port as the device used to send the message.

    ALEOS provides a message acknowledgment for every SMS message when it is passed to the radio. If ALEOS does not send an ACK, wait for 30 seconds, and then retry.

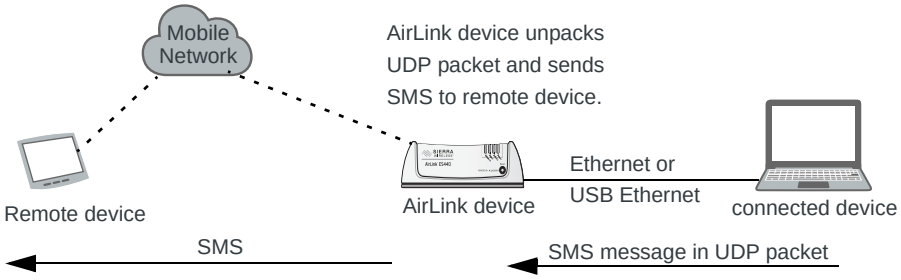
Security

12. If desired, configure SMS Security options (see SMS Security on page 211), SMS Wakeup (see SMS Wakeup on page 210), and Advanced options (see SMS > Advanced on page 214).
13. Click Apply.

    If you are using IP as the destination and you have changed the IPs or port numbers, reboot the device.

For information on the message format for an SMS Command, see Sending SMS Commands to an AirLink Device on page 199.

Sending a gateway message from a local IP device to a remote destination



The AirLink device acts as a gateway to send SMS messages from an IP connected device using AirLink SMS Protocol. The IP device sends a UDP packet to the AirLink device, which then sends the SMS to its destination.

Note: Outgoing SMS messages are limited to 140 characters.

To use AirLink SMS Protocol to send an SMS message from a connected device:

1. Begin with the start field.
2. Follow with the destination phone number. This number must be in the same format as the phone numbers in the Trusted Phone Number List.

Note: There is no space between the start number and the destination phone number or between any delimiter and the data fields.

3. Add the field delimiter.
4. Add the data type for the message:

For:	Enter:
ASCII	ASCII
8-bit	8BIT
Unicode	UCS-2
Data types are case sensitive.	

5. Add another field delimiter.
6. Add the number of ASCII characters in your original message (before it is converted to ASCII hex format).
7. Add another field delimiter.
8. Add the message to be sent in ASCII hex format. ASCII is case sensitive. Do not use any punctuation, such as a colon, or characters between hex pairs.

9. Finish with the end field.

   Example: You want to send the following message: “Test message” to phone number (510) 555-4200. To use this feature, convert the message to hex:54657374206d657373616765. Then format the message as follows:

   <<<15105554200,ASCII,12,54657374206d657373616765>>>

   where:
   - “<<<” is the start delimiter
   - “15105554200” is the phone number
   - “,” is the delimiter between fields
   - “ASCII” is the data type
   - “12” is the number of characters in the original message (before it is converted to ASCII hex format)
   - “54657374206d657373616765” is the message itself
   - “>>>” is the end delimiter

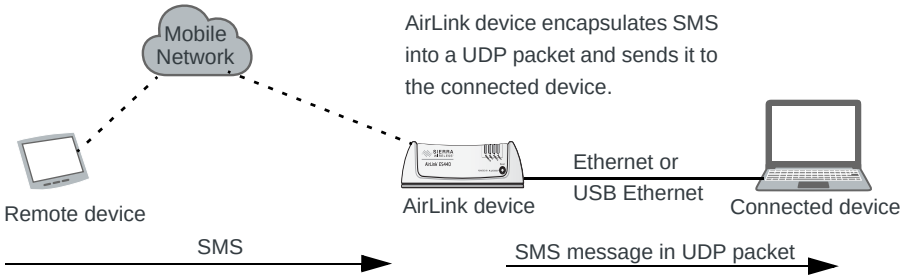
10. Send the UDP packet to the configured ALEOS port.

    After your message is sent, you receive an ACK message in the format ACK Field acknowledgment Code ACK Field. For example, if your message was successfully queued to be sent, you receive the message: ACK0ACK.

If you receive an error message, see SMS on page 453 for details.

*Note: You can also use AT*SMSM2M to send an SMS message to the remote device. For more information, see SMSM2M on page 216.*

Sending a gateway message to the connected device using IP address and port as the SMS destination


Mobile Network
AirLink device encapsulates SMS into a UDP packet and sends it to the connected device.
Ethernet or USB Ethernet
Remote device
AirLink device
Connected device
SMS
SMS message in UDP packet

Messages from a remote device can be sent to the AirLink device. The AirLink device encapsulates the message in a UDP packet using AirLink SMS Protocol, and sends it to the configured Local Host IP and Local Host Port on the connected device.

Message example:

Example:

1. An SMS is sent from phone number (640) 555-4200 to the device: “Test message”

2. The AirLink device receives the SMS and determines it is a gateway message.

3. The AirLink device converts the message into a UDP packet using the AirLink SMS Protocol and sends it to the configured Local Host IP at Local Host Port. The message as follows:

<<<16045554200,ASCII,12,54657374206d657373616765>>>

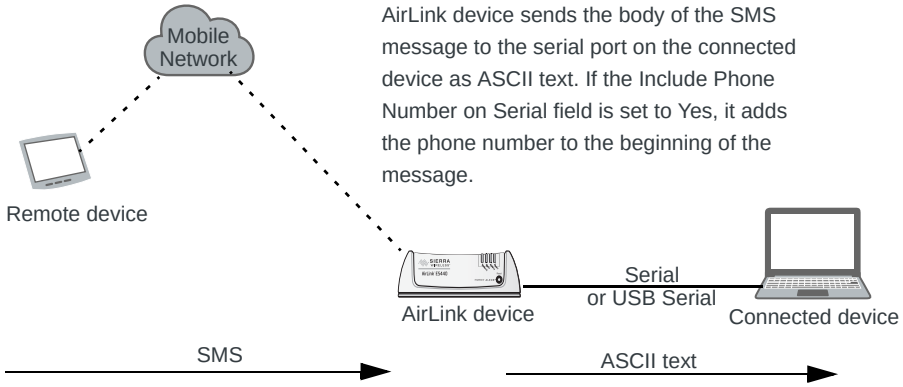
where:

- “<<<” is the start delimiter
- “16045554200” is the phone number
- “,” is the delimiter between fields
- “ASCII” is the message type*
- “12” is the number of characters in the message
- “54657374206d657373616765” is the message itself
- “>>>” is the end delimiter

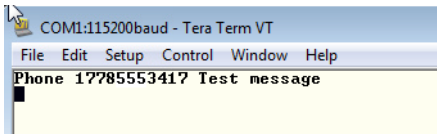
* In this example the message is in ASCII, but it could also be in 8-bit or Unicode format:

For:	Enter:
ASCII	ASCII
8-bit	8BIT
Unicode	UCS-2
Data types are case sensitive.	

Sending a gateway message to the connected device using Serial or USB Serial as the SMS destination


Mobile Network
AirLink device sends the body of the SMS message to the serial port on the connected device as ASCII text. If the Include Phone Number on Serial field is set to Yes, it adds the phone number to the beginning of the message.
Remote device
Serial or USB Serial
AirLink device
Connected device
SMS
ASCII text

A message can be sent from a remote device to the AirLink device. The AirLink device sends the body of the message in ASCII text to the connected device. If the Include Phone Number on Serial field is set to Yes, the AirLink device prepends the phone number to the message.



Control and Gateway

In Control and Gateway mode you can do both—send commands to the device and send gateway messages to the connected device. When the Trusted Phone Number List is enabled, all SMS messages from trusted devices that do not begin with the password indicator (PW) or the command prefix are sent to the connected device as a gateway message.

For more information, see Trusted Phone Number on page 212.

Configure ALEOS for Control and Gateway mode

1. In ACEmanager, go to Services > SMS.
2. Select Control and Gateway.

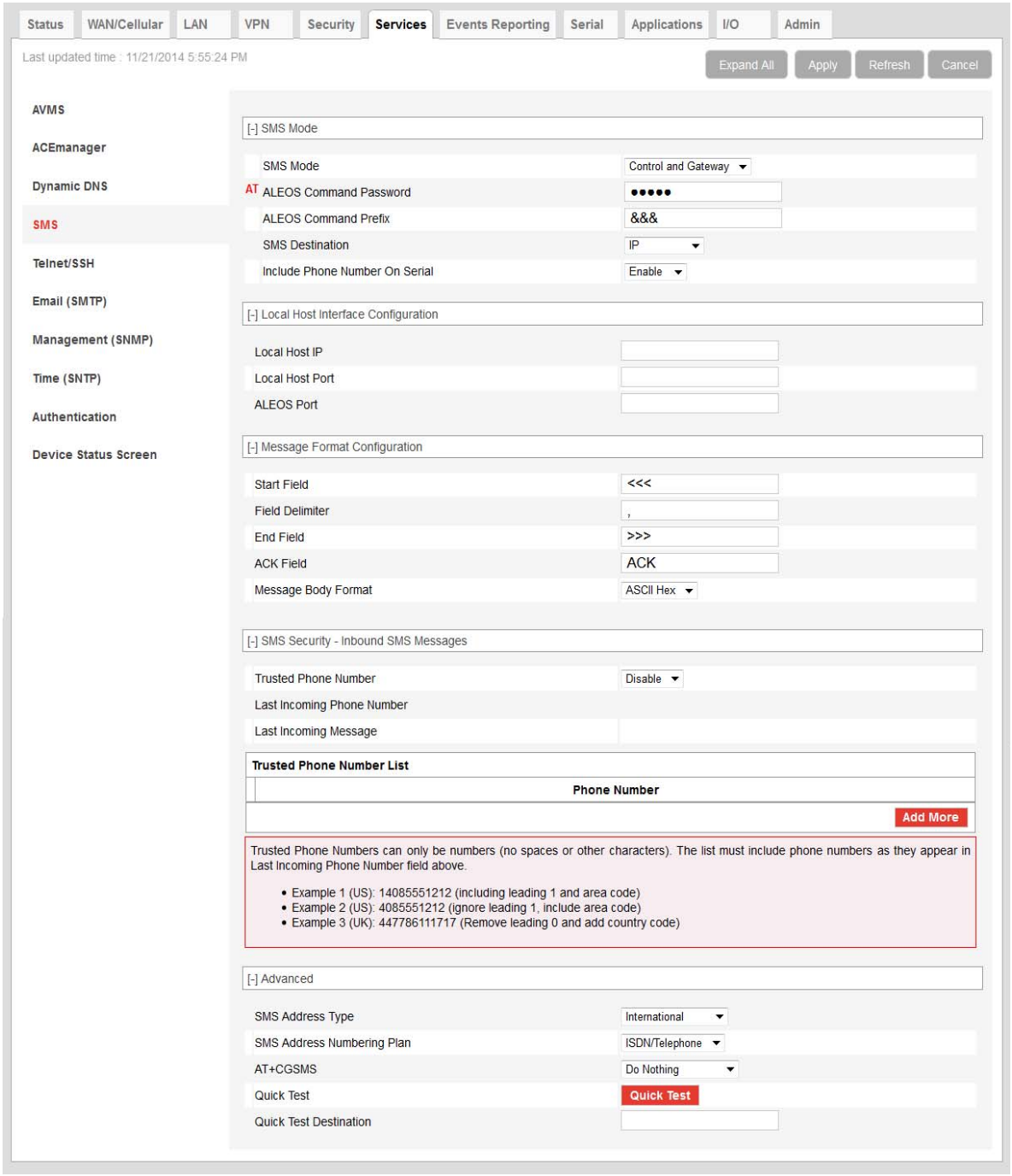


Figure 8-11: ACEmanager: Services > SMS (Control and Gateway)

For more information, see Control Only on page 201 and Gateway Only on page 202.

SMS Wakeup

This feature is supported on OpenSIM AirLink devices on the Vodafone network.

When the AirLink device is in Connect on traffic mode (for details, see Always on connection on page 82), you can configure the AirLink device to also initiate a mobile network data connection on receipt of an SMS. After the connection is established, it remains active until the configured timeout expires. The mobile network data connection closes after the specified timeout period. Outgoing traffic sent after the timer is triggered does not reset the timer.

To configure SMS Wakeup:

1. In ACEmanager go to WAN/Cellular > Advanced and ensure that the Always on connection field is set to Disabled - Connect on traffic.
2. Go to Services > SMS.

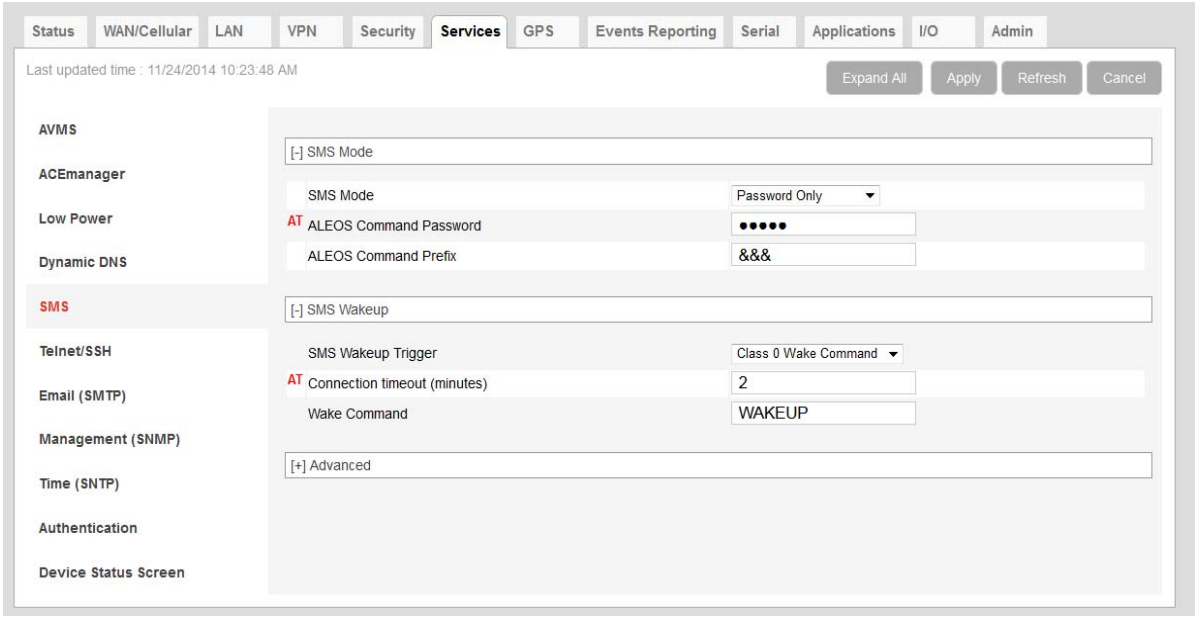


Figure 8-12: ACEmanager: Services > SMS

3. In the SMS Wakeup Trigger field, select the type of SMS that should wake up the device. The options are:
   - Feature Disabled
   - Any Class 0 message
   - Class 0 Wake Command
   - Any SMS message
   - Wake Command

Note: "Class 0 Wake Command" and "Wake Command" are SMS commands.

4. Click Apply.
5. In the Connection timeout (minutes) field, enter the number of minutes the mobile network data connection remains active after SMS Wakeup Trigger is received. Accepted values for this field are 2–65535. The default value is 2.

You can also set the Connection timeout using an AT command. For more information, see *SMSWUPTOUT on page 418.

6. If you selected Class 0 Wake Command or Wake Command in step 3, you can specify the SMS command name in the Wake Command field or use the default value, WAKEUP. Sending this SMS to the device will wake it up. Example: &&&WAKEUP (&&& is the SMS command prefix.)
7. Click Apply.

SMS Security

Inbound SMS Messages

Incoming SMS messages are received as UDP packets, and forwarded to the local device IP address and port. The UDP packets are in the same format as sent messages.

When Trusted Phone Number security is enabled, incoming messages coming from the phone numbers in the Trusted Phone Number list are the only ones for which commands will be performed (relay, response etc.) or gateway messages forwarded. Incoming messages from all other phone numbers will be ignored. Commands sent to the device with the correct password are always treated as coming from a trusted number.

All non-alphanumeric characters except a space will be replaced by a dot in ACEmanager.

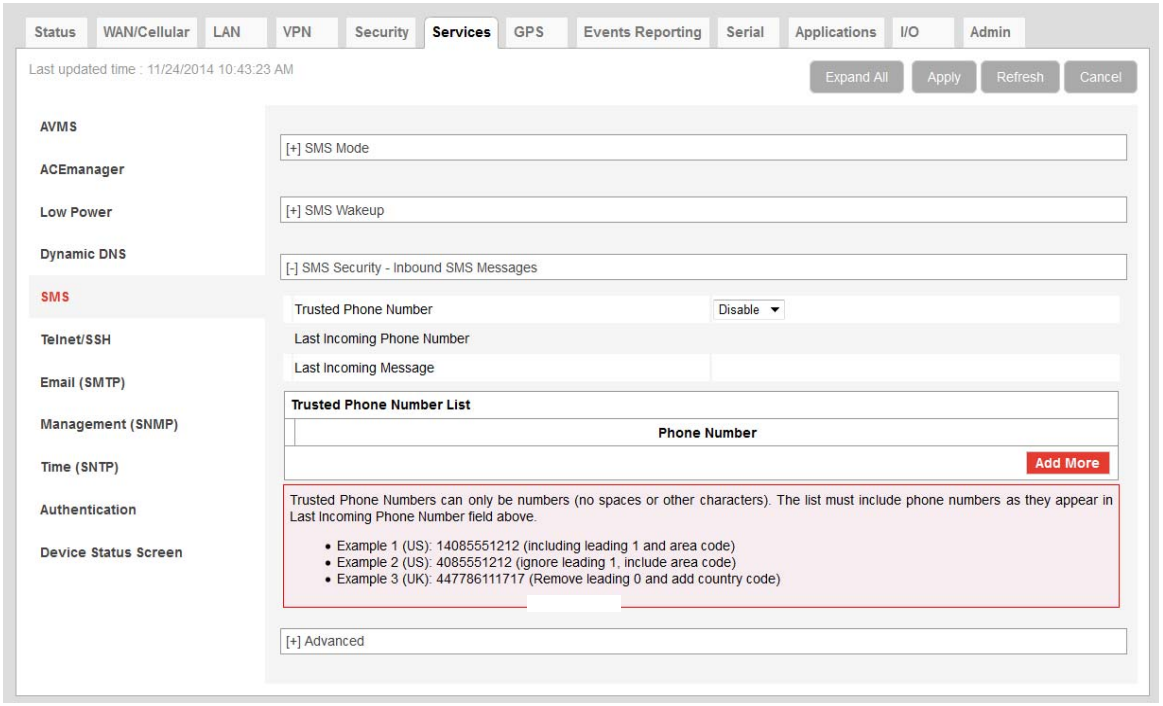


Figure 8-13: ACEmanager: Services > SMS

Field	Description
SMS Security - Inbound SMS Messages	
Trusted Phone Number	Allows you to Enable or Disable a trusted phone number
Last Incoming Phone Number	The last inbound phone number is displayed here. This will only be erased with a reset to defaults.
Last Incoming Message	The last incoming message is the last inbound SMS from the phone number. This will only be erased with a reset to defaults.
Trusted Phone Number List	Trusted phone numbers are listed here

Trusted Phone Number

Follow the instructions below to add a Trusted Phone Number on the SMS page.

1. Send an SMS command to the device, and hit Refresh. If Trusted Phone Number is enabled, and the phone number is not in the Trusted Phone Number List, no action is performed on the message.
2. Once you have the Last Incoming Phone Number that shows up on the SMS window in ACEmanager, note the exact phone number displayed.
3. Click Add More to add the Trusted Phone Number. The Last Phone Number will continue to display. Additions to the Trusted Phone Number become effective immediately. You do not need to reboot the device.

Note: The Trusted Phone number can be up to 15 characters long and must be comprised of numbers only.

Note: Phone Numbers (both trusted and not trusted) will be displayed in the Last Incoming Phone Number field.

4. Enter the Last Incoming Phone Number as the Trusted Phone Number.
5. Click Apply.

Note: Do not enter any extra digits, and use the Last Incoming display as a guide to type the phone number. Use “1” only if it is used in the beginning of the Last Incoming Phone Number.

With Trusted Phone Number enabled, only those SMS messages from Trusted Phone Numbers will receive responses to commands or messages acted on as applicable.

SMS Password Security

The SMS Password feature enables you to use a password to send a command at any time to the device. Even if Trusted Phone Number is enabled, you can send an SMS command from a non-trusted number, provided you include the password.

A default SMS password is generated from the last four characters of the SIM ID (for all SIM-based devices) or the ESN (for devices without a SIM, such those using EV-DO), or you can configure your own SMS password.

Tip: *If you do not know the SIM ID or ESN number you can find it in ACEmanager (Status > WAN/Cellular).*

Note: The SMS password is not the same as the ALEOS password used to access ACEmanager or Telnet/SSH.

To configure the SMS password:

1. Go to Services > SMS > SMS Mode.

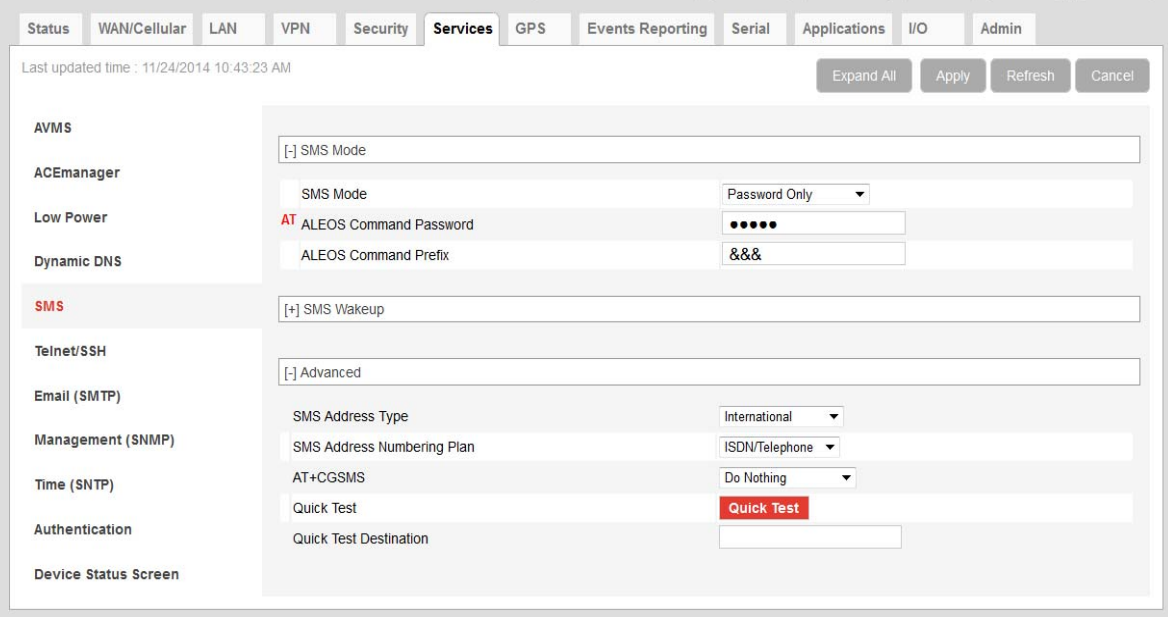


Figure 8-14: ACEmanager: Services > SMS >SMS Mode

2. Enter the desired SMS password in the ALEOS Command Password field.

   The password can be any alphanumeric string with a length between 1 and 255 characters.

3. Click Apply.

Note:

- *The SMS password is not displayed in plain text in ACEmanager. If you want to query it, use the AT command. See* *SMS_PASSWORD on page 417.*

- *The SMS password is not cleared by a configuration reset.*
- *If an SMS command is sent with the wrong SMS password, the device replies with a "Wrong Password" message, and the command is dropped.*

Using the Default SMS Password

You can use the default SMS password (last 4 characters of either the SIM ID number for SIM-based devices, or the ESN for devices without a SIM) with no prior configuration.

Note: The default password:

- *Works with all SMS commands*
- *Is not displayed in ACEmanager (If the ALEOS Command Password field is blank, the default password is used.)*
- *Is overridden by a user-defined password*
- *Changes if the SIM is changed, if no user-defined password is configured*

SMS > Advanced

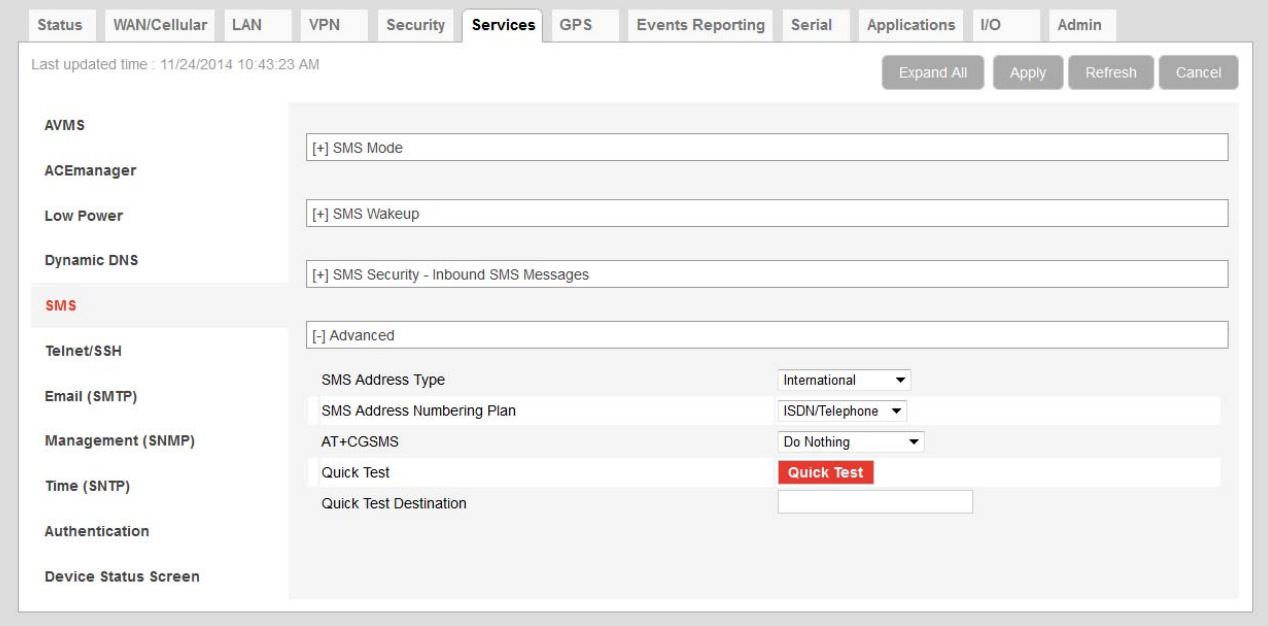


Figure 8-15: ACEmanager: Services > SMS > Advanced

Field	Description
SMS Address Type	For most networks, use the default setting (International). The address type of the phone number used to send outgoing messages and command responses. Options are: • International (default) • National • Network Specific • Subscriber • Abbreviated
SMS Address Numbering Plan	For most networks, use the default setting (ISDN/Telephone). The address numbering plan of the phone number used to send outgoing messages and command responses. Options are: • Unknown • ISDN/Telephone (default) • Date Numbering • Telex • National • Private • ERMES
AT+CGSMS	Allows you to choose the technology used to send SMS messages. For most networks, use the default setting (Do nothing). Options are: • Do nothing (default) • Set AT+CGSMS=0—GPRS • Set AT+CGSMS=1—Circuit switched • Set AT+CGSMS=2—GPRS Preferred (Uses circuit switched if GPRS is not available) • Set AT+CGSMS=3—Circuit Switched Preferred (Uses GPRS if circuit switched is not available) *Note: If your gateway is able to receive SMS messages, but is unable to send them, try changing this field to Set AT+CGSMS=1.* *Note: This field does not appear on CDMA/EV-DO devices or on LTE devices that fallback to CDMA/EV-DO.*
Quick Test	Allows you to send a test message to the destination entered in the Quick Test Destination field.
Quick Test Destination	Enter the phone number to use for the test message. Click Apply before clicking the Quick Test button. This field is cleared on reboot.

SMSM2M

SMS messages can be sent from the serial command interface. Enter AT*SMSM2M=”[phone] [message]”. The phone number needs to be in the same format as numbers entered in the Trusted Phone Number List.

The message must not exceed 140 characters. To send several messages back to back, you must wait for the OK before sending the next message.

Command	Description
***SMSM2M** ***SMSM2M_8** ***SMSM2M_u**	*SMSM2M is the command for ASCII text. *SMSM2M_8 is the command for 8-bit data. *SMSM2M_u is the command for unicode. Format: *smsm2m=”[phone][ascii message]” *smsm2m_8=”[phone][hex message]” *smsm2m_u=”[phone][hex message]” • The phone number can only consist of numbers (NO spaces or other characters). The phone number should be as it appears in the Last Incoming Phone Number field. Example 1 (US): 14085551212 (including leading 1 and area code) Example 2 (US): 4085551212 (ignore leading 1, include area code) Example 3 (UK): 447786111717 (remove leading 0 and add country code) Command Examples: *smsm2m=”18005551212 THIS IS A TEST” sends in ASCII. *smsm2m_8="17604053757 544849532049532041205445535 4" sends the message “THIS IS A TEST” as 8-bit data. *smsm2m_u="17604053757 000102030405060708090a0b0c0d0e0f808182838485868788898A8b8c8d8e8f" sends the bytes: 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f *Note: Not all cellular carriers support 8-bit or unicode SMS messages.*

Telnet/SSH

Use the Telnet or SSH protocol to connect to any AirLink device and send AT commands.

A secure mechanism to connect remote clients is a requirement for many users. In ACEmanager, Secure Shell (SSH) is supported to ensure confidentiality of the information and make the communication less susceptible to snooping and man-in-the-middle attacks. SSH also provides for mutual authentication of the data connection.

For information on configuring an AirLink device to use SSH or Telnet to access a connected serial device, see SSH PAD Mode on page 23.

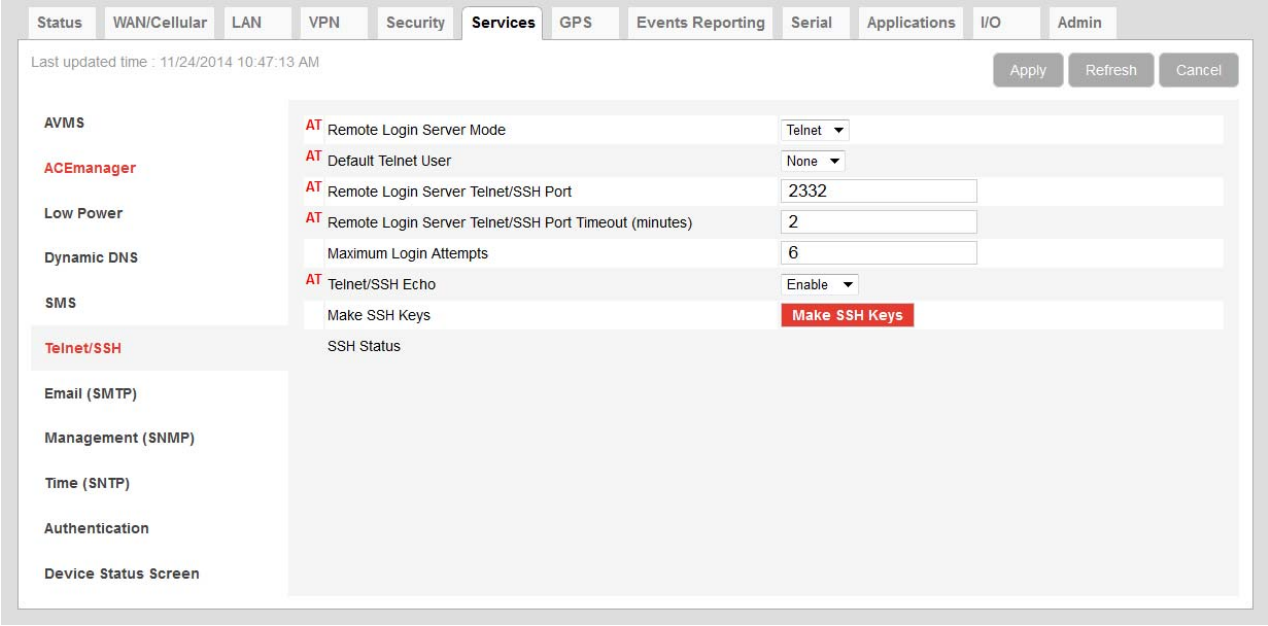


Figure 8-16: ACEmanager: Services > Telnet/SSH

Field	Description
Remote Login Server Mode	Select either Telnet (default) or SSH mode.
Default Telnet User	Select a default Telnet User name Options are: • None—When you log into a Telnet session, you are prompted for a user name and password. • user—When you log into a Telnet session, you are prompted only for a password. Telnet uses the default user name (user). *Note: The default user name is only for Telnet; not SSH.*

Field	Description
Remote Login Server Telnet/SSH Port	Sets or queries the port used for the AT Telnet/SSH server. Default: 2332 **Tip:** *Many networks have the ports below 1024 blocked. We recommend that you use a higher numbered port.*
Remote Login Server Telnet/SSH Port Timeout (mins)	Telnet/SSH port inactivity time out. Default: 2 (minutes)
Maximum Login Attempts	Sets the maximum number of login attempts. Default: 6
Telnet/SSH Echo	Enable (default) or disable AT command echo mode.
Make SSH Keys	Creates keys for SSH session applications
SSH Status	Provides the status of the SSH session

Note: When you are connected to SSH locally, you cannot have OTA SSH connected.

Email (SMTP)

For some functions, the device needs to be able to send email. Since it does not have an embedded email server, you need to specify the settings for a relay server for the device to use.

A reboot is required after configuring the email settings.

Note: The SMTP function will only work with a mail server that will allow relay email from the ALEOS device's Net IP.

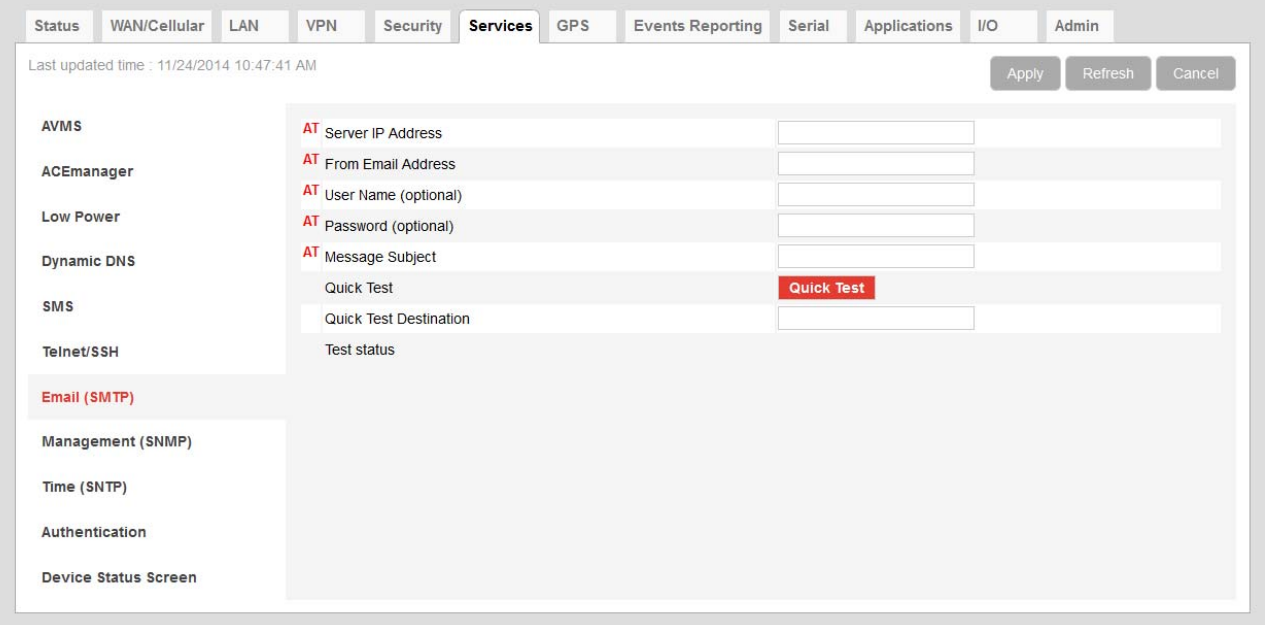


Figure 8-17: ACEmanager: Services > Email (SMTP)

Field	Description
Server IP Address	Specify the IP address or Fully Qualified Domain Name (FQDN) of the SMTP server to use. • d.d.d.d = IP Address • name = domain name (maximum: 40 characters)
From Email Address	Sets the email address from which the SMTP message is being sent. • email = email address (maximum: 30 characters)
User Name (optional)	Specifies the username to use when authenticating with the server
Password (optional)	Sets the password to use when authenticating the email account (*SMTPFROM) with the server (*SMTPADDR). • pw = password *Note: The email server used for the relay may require a user name or password.*
Message Subject	Allows configuration of the default Subject to use if one is not specified in the message by providing a “Subject: xxx” line as the initial message line. • subject = message subject

Management (SNMP)

The Simple Network Management Protocol (SNMP) is designed to allow for remote management and monitoring of a variety of devices from a central location. It is generally used to monitor conditions that may require attention.

The SNMP management system is composed of:

- One or more managers (administrative computers)
- SNMP-compliant devices (such as your AirLink device, a router, a UPS, a web server, a file server, or other computer equipment)
- An agent (data collection software running on the SNMP-compliant devices)
- A Network Management System (NMS) that monitors all the agents on a specific network.

The agent stores information about the device in a Management Information Base (MIB). The manager can send messages to this database to configure and query the status of the device. In addition, the agent running on the device can send traps (unsolicited messages) to the manager on startup, on status change, or when an error condition occurs.

AirLink devices supports SNMPv2c and SNMPv3 and you can configure them as SNMP agents.

Authentication ensures SNMP messages coming from the AirLink device have not been modified and the device cannot be queried by unauthorized users. SNMPv3 uses a User-Based Security Model (USM) to authenticate and, if desired or supported, message encryption. USM uses a user name and password specific to each device.

SNMPv2

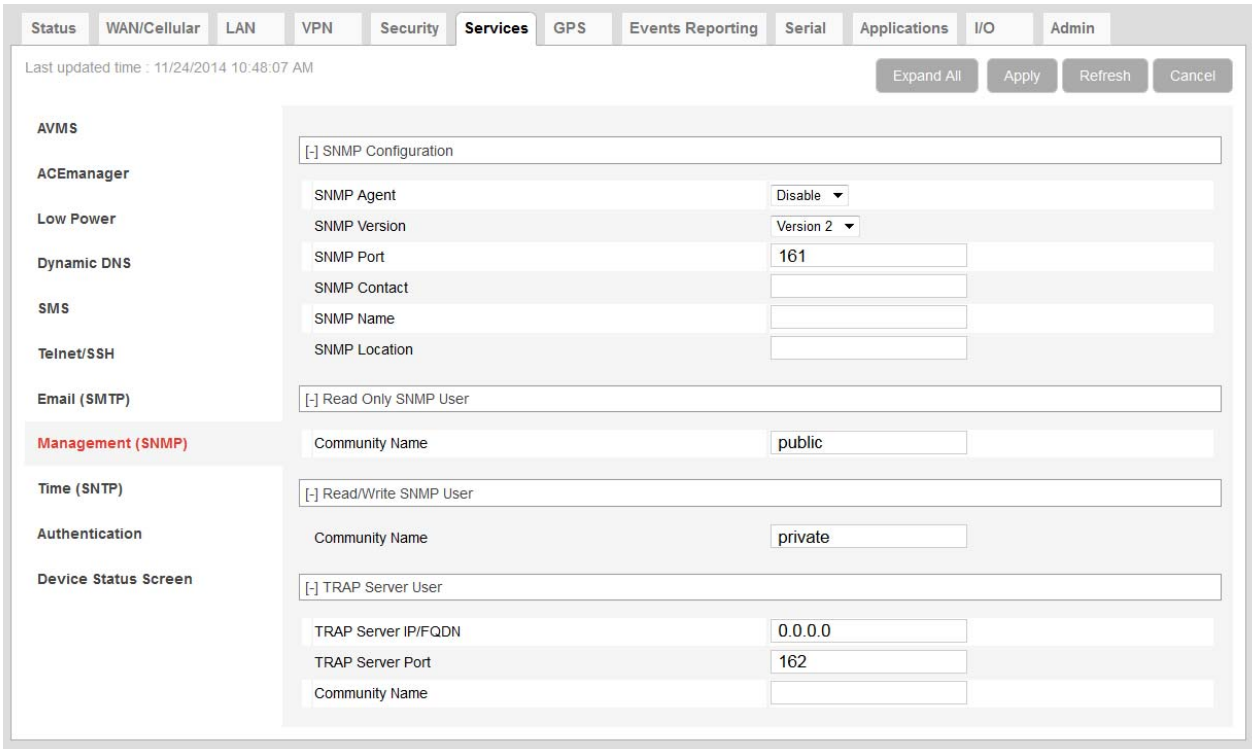


Figure 8-18: ACEmanager: Services> Management (SNMPv2)

Field	Description
SNMP Configuration	
Enable SNMP	Allows you to enable/disable SNMP Default: Disable
SNMP Version	Allows you to select either SNMP protocol Version 2 (default) or Version 3 communications.
SNMP Port	Controls which port the SNMP Agent listens on: • 1–65535 • Default is 161.
SNMP Contact	This is a personal identifier of the contact person you want to address queries to. This is a customer defined field.
SNMP Name	This is the name of the device you want to refer to. This is a customer defined field.
SNMP Location	Location of where your device is stored Enter a meaningful description of where the AirLink device is located.

Field	Description
Read Only SNMP User	
Community Name	The community name is a text string that acts as a password. It is used to authenticate messages that are sent between the management station and the device. Default is public.
Read/Write SNMP User	
Community Name	The community name is a text string that acts as a password. It is used to authenticate messages that are sent between the management station and the device. Default is private.
TRAP Server User	
TRAP Server IP/FQDN	Identifies the IP address or fully qualified domain name (FQDN) of the trap server that the AirLink device sends SNMP traps to
TRAP Server Port	Identifies the specific port the trap server is on • 1–65535 • Default is 162.
Community Name	The community name is a text string that acts as a password. It is used to authenticate messages that are sent between the management station and the device. There is no default value.

SNMPv3

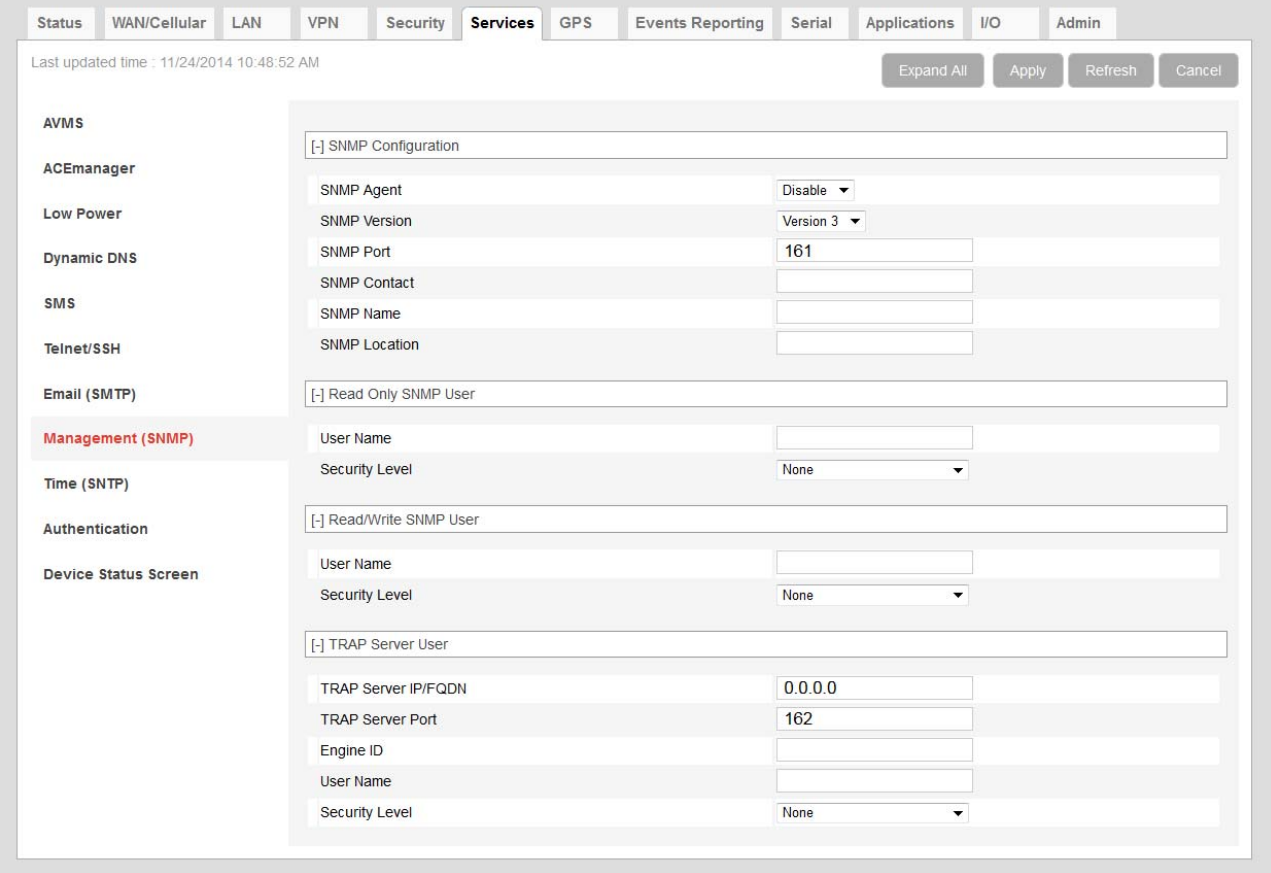


Figure 8-19: ACEmanager: Services> Management (SNMPv3)

Field	Description
SNMP Configuration	
Enable SNMP	Allows you to enable/disable SNMP Default is Disable.
SNMP Version	Allows you to select either SNMP protocol Version 2 (default) or Version 3 communications.
SNMP Port	Controls which port the SNMP Agent listens on: • 1 – 65535 • Default is 161.
SNMP Contact	This is a personal identifier of the contact person you want to address queries to. This is a customer defined field.
SNMP Name	This is the name of the device you want to refer to. This is a customer defined field.
SNMP Location	Location of where your device is stored. This is a customer defined field.

Field	Description
Read Only SNMP	
User Name	Allows these SNMP users to view, but not change the network configuration
Security Level	Security types available: None, Authentication Only, and Authentication and Privacy.
Authentication Type	Authentication types available: MD5 or SHA *Note: This field is only available when you select either Authentication and Privacy, or Authentication Only in the Security Level field.*
Authentication Key	This key authenticates SNMP requests for SNMPv3. • Minimum length: 8 ASCII characters • Maximum length: 255 ASCII characters Example: My Key_1234 *Note: This field is only available when you select either Authentication and Privacy, or Authentication Only in the Security Level field.*
Privacy Type	Privacy types available: AES or DES *Note: This field is only available when you select Authentication and Privacy in the Security Level field.*
Privacy Key	This key ensures the confidentiality of SNMP messages via encryption • Minimum length: 8 ASCII characters • Maximum length: 255 ASCII characters Example: My Key_56789 *Note: This field is only available when you select Authentication and Privacy in the Security Level field.*
Read/Write SNMP For a description of the Read/Write SNMP fields, see Read Only SNMP on page 224.	
TRAP Server User	
TRAP Server IP/FQDN	Identifies the IP address or fully qualified domain name (FQDN) of the trap server that the AirLink device sends SNMP traps to
TRAP Server Port	Identifies the specific port the trap server is on • 1 – 65535 • Default is 162.

Field	Description
Engine ID	The Engine ID is a mandatory field that uniquely identifies the SNMPv3 agent in the device to the server. The Engine ID is 5–32 octets long (1 octet is 2 hex characters). That is: • Minimum length: 10 hex characters • Maximum length: 64 hex characters Create the engine ID by entering hex characters only, with no leading 0x. For example, ABCDEF1020
User Name	See User Name on page 224.
Security Level	See Security Level on page 224.
Authentication Type	See Authentication Type on page 224.
Authentication Key	See Authentication Key on page 224.
Privacy Type	See Privacy Type on page 224.
Privacy Key	See Privacy Key on page 225.

Time (SNTP)

The device can be configured to synchronize its internal clock with a time server on the Internet using the Simple Network Time Protocol. Normally your device will synchronize with the cellular network or GPS.

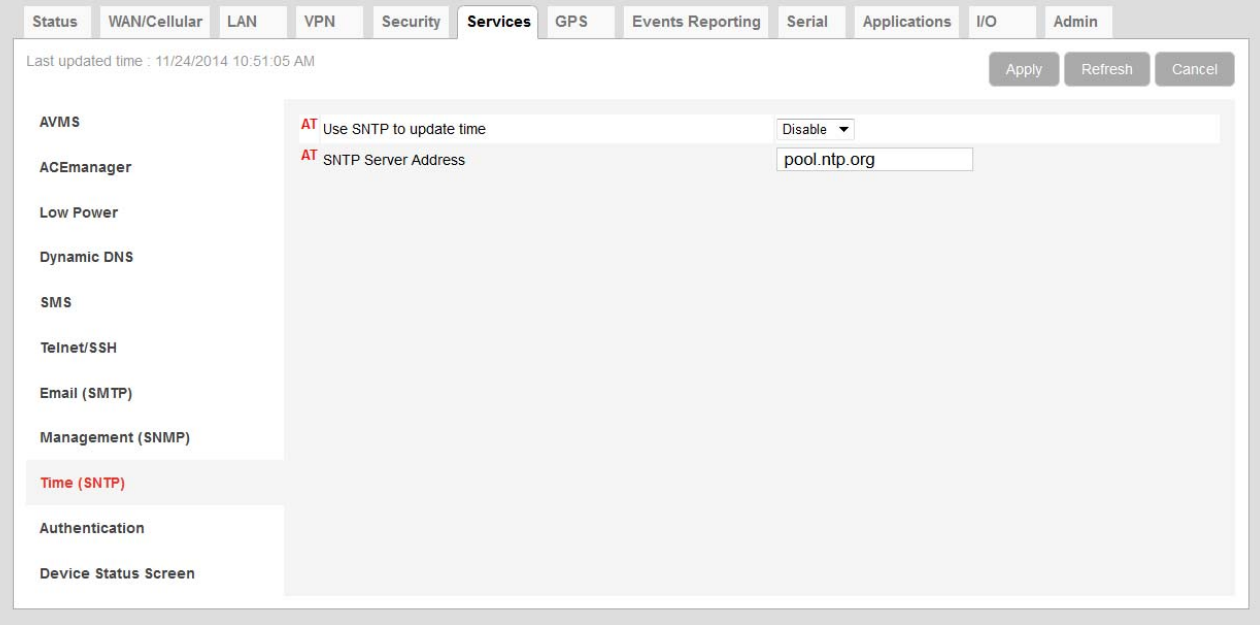


Figure 8-20: ACEmanager: Services > Time (SNTP)

Field	Description
Enable time update	Enables daily SNTP update of the system time. Default: Disable
SNTP Server Address	SNTP Server IP address, or fully qualified domain name, to use if *SNTP=1. If blank, time.nist.gov is used. • d.d.d.d=IP address • name=domain name

Authentication

ALEOS supports ACEmanager login using secure LDAP, RADIUS, and TACACS+ authentication schemes. This enables enterprise IT managers to centrally manage access to AirLink devices and produce an audit trail showing which users logged into specific devices and when.

Note the following:

- You can configure any or all of these schemes at the same time. When more than one scheme is configured, the authentication is successful if at least one of the schemes authenticates the user.
- Successful authentication can take time. For example, if you have all three authentication schemes enabled, ALEOS first attempts to reach the LDAP server. If it is unable to reach the LDAP server in the configured timeout period, it abandons the attempt and tries to reach the RADIUS server. If that server is unreachable after the timeout period, it then tries to reach the TACACS+ server. If none of the servers are reachable in the configured timeout periods, ALEOS falls back to ACEmanager user name and password authentication.
- LDAP, RADIUS, and TACACS+ provide authentication (checks the user's credentials) but do not check authorization (account expiration date, user rights, etc.) All users authenticated using the LDAP, RADIUS, and TACACS+ servers have administrative rights (i.e. a user account, not a viewer account) and can modify the AirLink device settings. Ensure that LDAP, RADIUS, and TACACS+ users are authorized to modify device settings.
- LDAP, RADIUS, and TACACS+ are supported for ACEmanager logins, but are not supported by other AirLink device services such as Telnet, SSH, PPPoE, etc.

For instructions on configuring these authentication schemes, see:

- LDAP Authentication on page 227
- RADIUS Authentication on page 228
- TACACS+ Authentication on page 229

LDAP Authentication

Lightweight Directory Access Protocol (LDAP) is a network protocol for accessing and manipulating information stored in a directory. It is suitable for using with information that must be easily available and accessible, and does not change frequently. AirLink devices support LDAP version 3.

To configure LDAP:

1. Go to Services > Authentication.
2. In the LDPA Client field, select Enable.

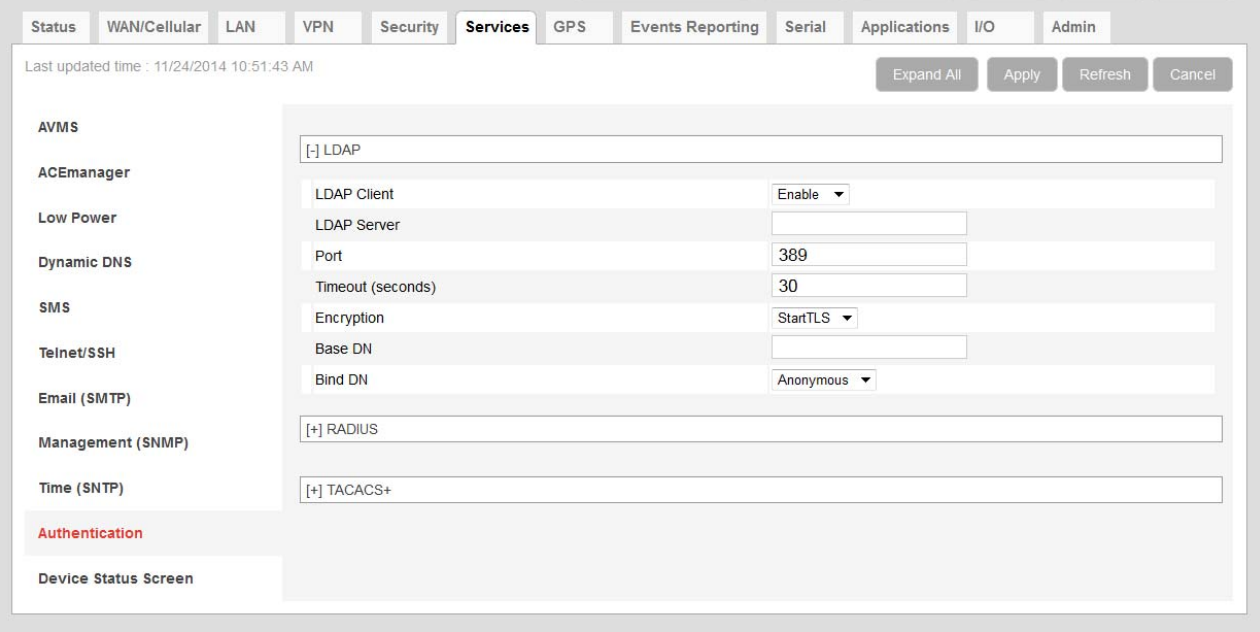


Figure 8-21: ACEmanager: Services > Authentication > LDAP

3. Configure the other fields as described in the following table.

Field	Description
LDAP Server	LDAP server IP address or resolvable domain name
Port	By default, LDAP uses TCP port 389
Timeout (seconds)	The time limit for the server to respond • 1–60 seconds Default is 30 seconds. *Note: If the server does not respond during the timeout (no route to host, server down, network too slow etc.), the authentication fails and the next enabled authentication mechanism checks the credentials.*

Field	Description
Encryption	Select the encryption type Options are: • None • SSL—Secure Sockets Layer protocol —Non-standard legacy (pre-LDAPv3) encryption type • StartTLS—Secure mechanism integrated into the LDAPv3 protocol (default)
Base DN	Distinguished name of the search base
Bind DN	Choose how the LDAP search is done Options are: • Anonymous—Bind anonymously (default) • Explicit—Use a specific account to bind with
Bind DN User	This field only appears if you selected Explicit in the Bind DN field User name to bind with
Bind on Password	This field only appears if you selected Explicit in the Bind DN field User password to bind with

4. Click Apply.

RADIUS Authentication

Remote Authentication Dial In User Service (RADIUS) uses UDP and checks authentication credentials, using a shared key.

To configure RADIUS:

1. Go to Services > Authentication.
2. In the RADIUS Client field, select Enable.

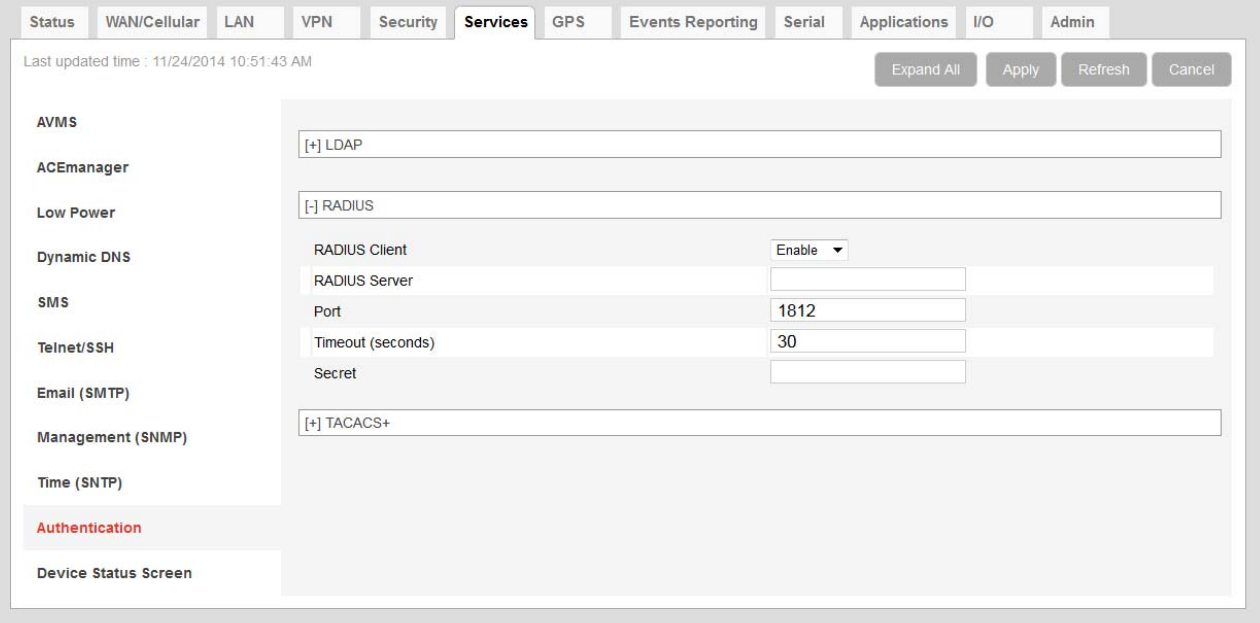


Figure 8-22: ACEmanager: Services > Authentication > RADIUS

3. Configure the other fields as described in the following table.

Field	Description
RADIUS Server	RADIUS server IP address or resolvable domain name
Port	By default, RADIUS uses UDP port 1812
Timeout (seconds)	The time limit for the server to respond • 1–60 seconds Default is 30 seconds. *Note: If the server does not respond during the timeout (no route to host, server down, network too slow etc.), the authentication fails and the next enabled authentication mechanism checks the credentials.*
Secret	Shared secret for configured server

4. Click Apply.

TACACS+ Authentication

Terminal Access Controller Access-Control System Plus (TACACS+) uses TCP protocol and encrypts the entire packet, except the header.

To configure TACACS+:

1. Go to Services > Authentication.

2. In the TACACS+ Client field, select Enable.

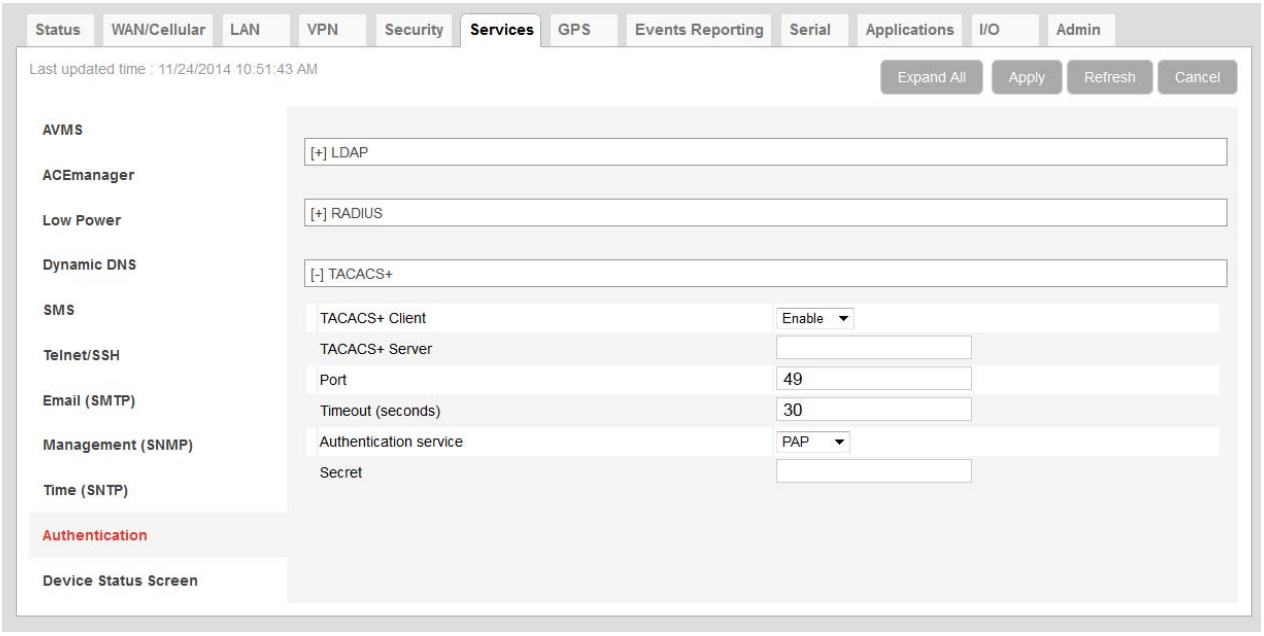


Figure 8-23: ACEmanager: Services > Authentication > TACACS+

3. Configure the other fields as described in the following table.

Field	Description
TACACS+ Server	TACACS+ server IP address or resolvable domain name
Port	By default, TACACS+ uses TCP port 49
Timeout (seconds)	The time limit for the server to respond • 1–60 seconds Default is 30 seconds. *Note: If the server does not respond during the timeout (no route to host, server down, network too slow etc.), the authentication fails and the next enabled authentication mechanism checks the credentials.*
Authentication service	The type of bind used for authentication Options are: • PAP—Password Authentication Protocol (default) • CHAP— Challenge Handshake Authentication Protocol The stronger of the two protocols. Recommended, provided it is supported by all the client devices. • Login—User name and password
Secret	Shared secret for configured server

4. Click Apply.

Device Status Screen

The Device Status Screen feature, when enabled, allows you to add GPS and network status parameters to the ACEmanager Login screen. Once enabled, subsequent logins to ACEmanager display whatever status parameters have been previously checked on the Device Status Screen.

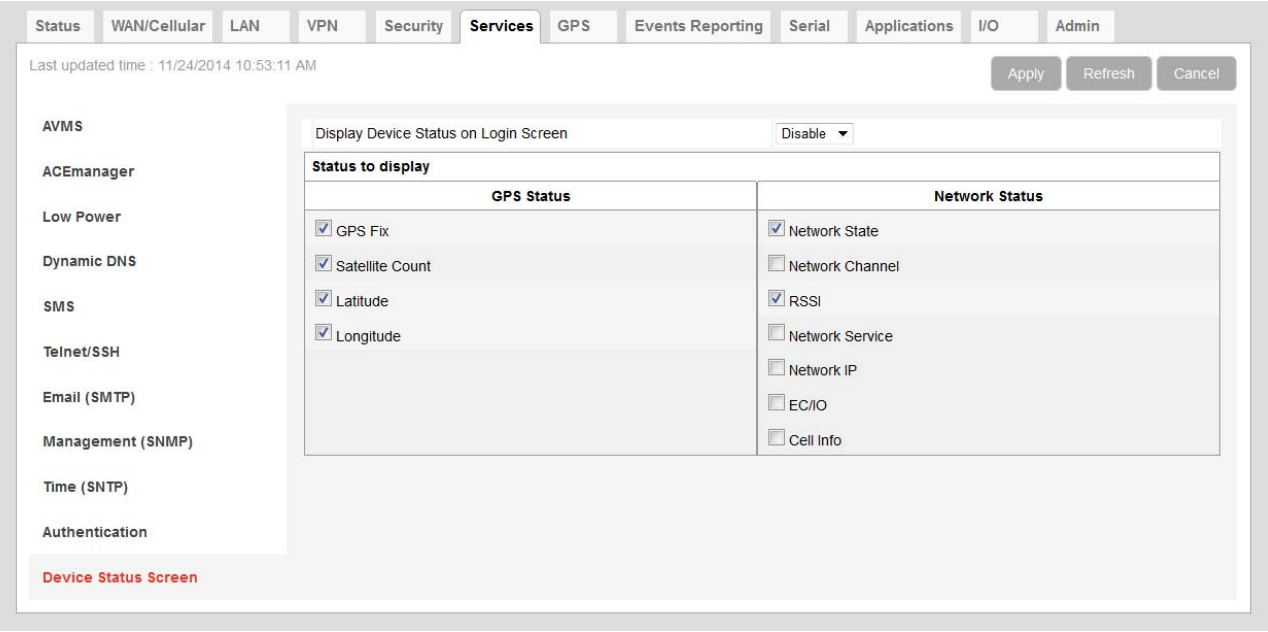


Figure 8-24: ACEmanager: Services > Device Status Screen

Field	Description
Enable Device Status on Login Screen	Enables device status parameters on the login screen Options are: Disable or Enable (default)
Status to display	Allows you to display specific GPS and network status parameters on the login screen

9: GPS Configuration

9

Most AirLink devices are equipped with a Global Positioning System receiver (GPS) to ascertain its position and track the movements of a vehicle or other devices which move. The AirLink device relays the information of its location as well as other data for use with tracking applications.

GPS Overview

The Global Positioning System (GPS) is a satellite navigation system used for determining a location and providing a highly accurate time reference.

GPS consists of a "constellation" of 32 satellites in 6 orbital planes. Each satellite circles the Earth twice every day at an altitude of 20,278 kilometers (12,600 miles). Each satellite is equipped with an atomic clock and constantly broadcasts the time, according to its own clock, along with administrative information including the orbital elements of its motion, as determined by ground-based observatories.

A GPS receiver, such as the AirLink device, requires signals from four or more satellites and performs Time Difference of Arrival (TDoA) calculations in order to determine its own latitude, longitude, and elevation.

The GPS data can then be transmitted to a server with a tracking application to compile information about location, movement rates, and other pertinent data.

Note: Depending on the location of the satellites in relation to the device's location and how many signals are being received, the AirLink device may encounter "GPS drift", a phenomenon whereby a stationary device is reported as moving by the GPS system. This "drift" is within the location tolerances of the GPS system, but the device may appear to be moving, based on continuous GPS calculations.

Common Uses for GPS

- Driver navigation—The AirLink device provides real time GPS data via the serial or Ethernet port to a local application, including applications that provide mapping and navigation support.
- Automatic Vehicle Location (AVL)—The AirLink device provides real time GPS data to the server that tracks the location and other variables of the vehicle or asset.

ALEOS Supported GPS Report Protocols

- Remote Access Protocol (RAP)

  RAP is a proprietary binary message format developed and maintained by Sierra Wireless and used by many 3rd party applications. Because it is designed and maintained by Sierra Wireless, RAP supports more ALEOS features than other GPS protocols. It is a low-byte-usage protocol that can be used to develop low cost AVL solutions.

  The RAP messages are in hex and are referred to by their message ID. Reports can include GPS data alone, as well as GPS data with the date and time, radio frequency data, radio status information, and I/O state changes, and power state changes. For an example, see GPS RAP Report Sequence Example on page 245. For more information, contact your Sierra Wireless Sales representative for information on how to obtain a copy of the RAP Protocol Guide.
- National Marine Electronics Association (NMEA®)

  NMEA is an ASCII protocol used by many GPS tracking applications.
- Trimble® ASCII Interface Protocol (TAIP)

  TAIP is a digital communication interface based on printable ASCII characters over a serial data link. TAIP was designed specifically for vehicle tracking applications but has become common in a number of other applications, such as data terminals and portable computers, because of its ease of use.
- Xora®

  Protocol specific to Xora asset management and tracking applications

Before Configuring GPS

To decide what configuration you need for your AirLink device, there are some fundamental considerations you should determine:

- **Protocol—**What is the GPS protocol used by your tracking application and what type of reports will you need? (See GPS Report Type on page 240.)
- **Dynamic IP Address—**Does your device have a dynamic IP address and you need to track the specific asset? (See Device ID in Local Reports on page 252.) You can also associate your device with a dynamic DNS configuration. (See Dynamic DNS on page 191.)
- **Server location and type of connection—**Will you be using a local server, a remote server, or both? Will you need a serial or local IP connection? (See Figure 9-1 on page 235 for information.)
- **Multiple GPS servers—**Will you need to have GPS data sent to more than one GPS server?

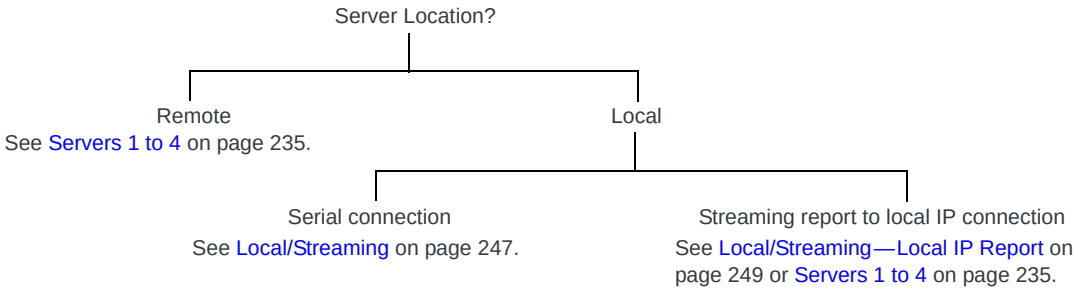

Server Location?
Remote
See Servers 1 to 4 on page 235.
Local
Serial connection
See Local/Streaming on page 247.
Streaming report to local IP connection
See Local/Streaming—Local IP Report on page 249 or Servers 1 to 4 on page 235.

Figure 9-1: Server location and connection type

Note: Most Global settings (described on page 253) apply to remote and local servers. All GPS configuration changes go into effect immediately. No reboot of the AirLink device is necessary. After you configure any settings there is a short pause in receiving GPS reports while the device is re-initialized with the new configuration.

Servers 1 to 4

You can configure up to four servers as report destinations. Each server is configured independently and can be configured to report the same or different information. This enables you to simultaneously receive GPS and other information at more than one location, either local or remote.

The configuration fields are the same for each of the four servers, except that Server 1 has the option to configure one or two redundant servers.

Note: These side tabs only appear if GPS Service (on the Global Settings side tab) is Enabled.

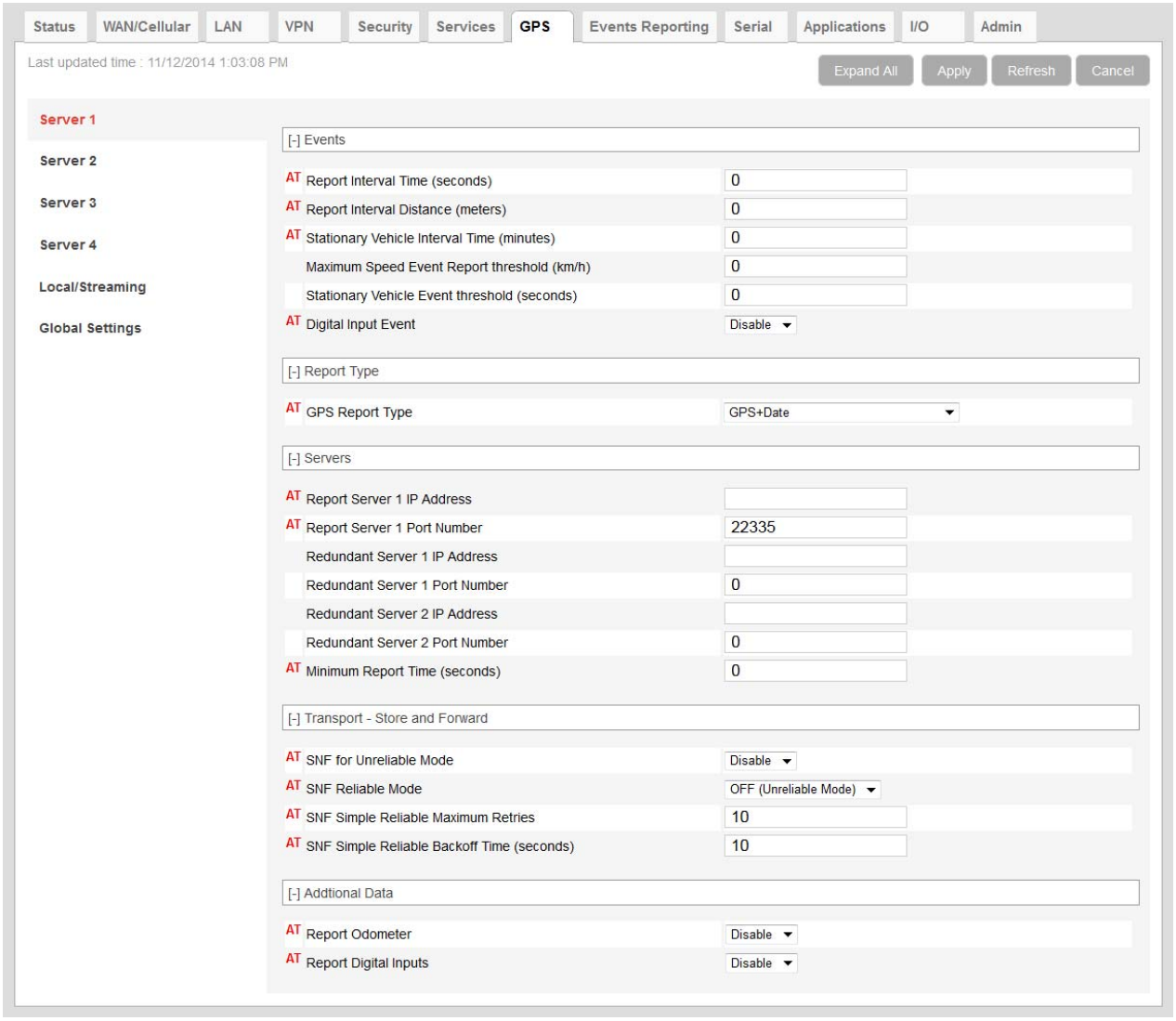


Figure 9-2: ACEmanager: GPS > Server 1

Table 9-1: GPS: Servers 1–4

Field	Description
Events—Configure when the GPS reports are sent	
Report Interval Time (seconds)	GPS Report Time Interval The amount of time between GPS reports (in seconds) Options are: • 1– 65535 • 0 = Disables GPS reporting based on a time interval (default) With this option disabled, you can still receive reports based on distance traveled or the vehicle being stationary for a configured time. (See Report Interval Distance (meters) on page 237 and Stationary Vehicle Timer (minutes) on page 238.) You can also use an AT Command to set this value. For more information, see *PPTIME on page 428. *Note: Your cellular carrier may impose a minimum transmit time.*
Report Interval Distance (meters)	GPS Report Distance Interval in meters The distance (in meters) that the vehicle (or device) travels between sending GPS reports Options are: • 40– 65535 Note that setting the resolution near the low end of the range may result in incorrect reports as a result of GPS jitter (i.e. apparent motion caused by the inherent inaccuracy in GPS measurements). • 0 = Disables sending GPS reports based on a distance interval (default) With this option disabled, you can still receive reports based on time passed or the vehicle being stationary for a configured time. (See Report Interval Time (seconds) on page 237 and Stationary Vehicle Timer (minutes) on page 238.) You can also use the AT Command, *PPDISTM, to set this value. For more information, see page 424. *Note: An an additional AT Command, *PPDIST, allows you to configure the GPS report distance interval in 100 meter units. This option is only available through AT Commands. For more information, see page 423.* *Note: If the report interval time and report interval distance fields are both set, GPS reports are sent when either interval is reached. For example, if the time interval is reached, a GPS report is sent even if the distance is not reached. Conversely, if the vehicle travels the specified distance, a GPS report is sent even if the time interval was not reached.*

Table 9-1: GPS: Servers 1 – 4

Field	Description
Stationary Vehicle Timer (minutes)	You can use this field if you want to receive less frequent reports when the vehicle is stationary. A GPS report is sent every x minutes the vehicle (or device) is stationary, where x is the value configured in this field. When the vehicle is stationary, this value overrides the value configured in the Report Interval Time field. Options are: • 1–255 • 0 = Disables GPS reporting based on a vehicle being stationary (default) You can also use an AT Command to set this value. For more information, see *PPTSV on page 428.
Maximum Speed Event Report (km/h)	A GPS report is sent if the speed (in kilometers per hour) configured in this field is exceeded, and again when the speed goes back down below the configured value. • 0 = Disable (default) • 1–255 *Note: If you are using one of the RAP GPS report types (see GPS Report Type on page 240) the GPS report triggered by this feature includes:* • *A marker to indicate that it was triggered by the configured speed being exceeded and when the speed is goes back down below the configured value.* • *The standard GPS information for the configured report type* *For more information, refer to the RAP Protocol Guide.* *If you are not using a RAP GPS report, a standard report is sent.*
Send Stationary Vehicle Event in Seconds	A GPS report is sent if the vehicle (or device) has been in one location for more than the specified time (in seconds) and again when the vehicle (or device) moves from that location. Options are: • 1–255 • 0 = Disables sending GPS reports based on a vehicle being stationary (default) *Note: If you are using one of the RAP GPS report types (see GPS Report Type on page 240) the GPS report triggered by this feature includes:* • *A marker to indicate that it was triggered by the vehicle either being stationary or starting to move again* • *The standard GPS information for the configured report type* *For more information, refer to the RAP Protocol Guide.* *If you are not using a RAP GPS report, a standard report is sent.* You can configure Stationary Vehicle Event in Seconds and Stationary Vehicle Timer together to receive a special report when the device is stationary longer than x seconds, a normal report every x minutes it is stationary (instead of the Report Interval Time) and a special report when the vehicle begins moving again.

Table 9-1: GPS: Servers 1 – 4

Field	Description
Enable Digital Input Event	A GPS report is sent if the configured digital input changes. For example, this could be used to trigger a report being sent when an emergency light or siren is turned on or off, or when a door is opened or closed. The GPS data in the report informs you of where the event took place. Options are: • Disable (default) • Enable *Note: If you are using one of the RAP GPS report types (see GPS Report Type on page 240) the GPS report triggered by this feature includes:* • *A marker to indicate that it was triggered by a change in status of the configured digital input* • *The standard GPS information for the configured report type* *For more information, refer to the RAP Protocol Guide.* *If you are not using a RAP GPS report, a standard report is sent.* You can also use an AT Command to set this value. For more information, see *PPINPUTEVT on page 425.

Table 9-1: GPS: Servers 1 – 4

Field	Description
Report Type	
GPS Report Type	Sets the type of GPS Report Options are: RAP • GPS Data—RAP GPS report that contains only GPS data • GPS+Date—RAP GPS report that contains GPS data with the UTC time and date (default) • GPS+Date+RF—RAP GPS report that contains GPS data, the UTC time and date, and radio frequency information for the cellular connection • GPS+Date+RF+EIO—RAP GPS report that contains GPS data, the UTC time and date, radio frequency information for the cellular connection, and the current I/O state NMEA • NMEA GGA+VTG—NMEA GPS report that contains fix information, vector track, and speed over ground • NMEA GGA+VTG+RMC—NMEA GPS report that contains fix information, vector track, speed over ground, and recommended minimum GPS data • NMEA GGA+VTG+RMC+GSA+GSV—NMEA GPS report that contains fix information, vector track, speed over ground, the recommended minimum GPS data, overall satellite data, and detailed satellite data TAIP • TAIP data—TAIP GPS report that contains position and velocity • Compact TAIP data—TAIP GPS report that contains the compact position • TAIP LN report—TAIP GPS report that contains a long navigation message • TAIP TM report—TAIP GPS report that contains the time and date XORA • XORA data—GPS report used with Xora asset tracking *Note: Only RAP GPS reports can be configured to include odometer and digital I/O information.* *Note: You can also use an AT Command to set this value. For more information, see *PPGPSR on page 425.*

Table 9-1: GPS: Servers 1 – 4

Field	Description
Servers—Configure where the reports are sent	
Report Server IP Address	IP address or FQDN (fully qualified domain name) of the server where GPS reports are sent Example: 192.100.100.100 The IP address can be for a local host or a remote server that is accessed over-the-air or via a VPN tunnel. If an IP with the last octet of 255 is configured (i.e. 192.168.13.255), a report would be broadcast to all IPs on that subnet. When configured to a local host subnet, any connected host would receive the report. *Note: If you want to use it as a LAN host, it must have a private IP address. If you want to use a public IP address, use a Local IP report. (See Local/Streaming—Local IP Report on page 249.)* You can also use an AT Command to set this value. For more information, see *PPIP on page 425.

Table 9-1: GPS: Servers 1 – 4

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Report Server Port Number</td><td>
Destination port on the server where GPS reports are sent
The destination port can be the same for all servers or you can configure a different destination port for each server. Options are: 1–65535
Defaults:
• Server 1 destination port: 22335
• Server 2 destination port: 22336
• Server 3 destination port: 22337
• Server 4 destination port: 22338
You can also use an AT Command to set these values. For more information, see *PPPORT on page 427.
Note: If the account is behind a firewall (for example, an account that is not Internet-routable), the report may be redirected to come from a different source port when it arrives at the server.
The source ports on the device are not configurable. The following source ports are used:
<table>
<tr><th>Protocol</th><th>Server</th><th>Port</th></tr>
<tr><td rowspan="4">RAP/NMEA</td><td>1</td><td>17335</td></tr>
<tr><td>2</td><td>17345</td></tr>
<tr><td>3</td><td>17346</td></tr>
<tr><td>4</td><td>17347</td></tr>
<tr><td rowspan="4">TAIP</td><td>1</td><td>21000</td></tr>
<tr><td>2</td><td>21001</td></tr>
<tr><td>3</td><td>21002</td></tr>
<tr><td>4</td><td>21003</td></tr>
<tr><td rowspan="4">XORA</td><td>1</td><td>9494</td></tr>
<tr><td>2</td><td>9495</td></tr>
<tr><td>3</td><td>9496</td></tr>
<tr><td>4</td><td>9497</td></tr>
</table>
</td></tr>
</table>

Table 9-1: GPS: Servers 1 – 4

Field	Description
Redundant Servers — Only available for Server 1 If the redundant server is configured, anytime a report is sent to server 1, an identical report is sent to any configured redundant server(s). Transport/SNF configuration settings do not apply to redundant servers. Commands from redundant servers are ignored. Reports originate from port 17335. The redundant servers can be a local host or a remote server that is accessed over-the-air or via a VPN tunnel.	
Redundant Server 1 IP Address	IP address or FQDN of the first redundant server
Redundant Server 1 Port Number	Port number of the first redundant server The port number can be the same as or different from that of other servers.
Redundant Server 2 IP Address	IP address or FQDN of the second redundant server
Redundant Server 2 Port Number	Port number of the second redundant server The port number can be the same as or different from that of other servers.
Minimum Report Time (secs)	Specifies the minimum time (in seconds) between partial reports or grouped packets being sent You can also use an AT Command to set this value. For more information, see *PPMINTIME on page 426.
Transport / Store and Forward (SNF) — This feature is designed to accommodate periods when the AirLink device is outside the area of cellular network coverage or otherwise unable to reach the report server. Reports are stored and then "forwarded" in a combined packet when the device is again able to contact the server.	
Enable SNF for Unreliable Mode	Store and Forward causes GPS reports to be stored if the AirLink Device goes out of network coverage. Once the device/vehicle is in coverage the stored GPS reports are sent to the server. Options are: • Disable (default)—If there is no cellular network coverage, reports are not stored. • Enable—If there is no cellular network coverage, reports are stored until the AirLink device can access the server. *Note: When you are using GPS and Wi-Fi Client mode: If the Wi-Fi client is connected, reports are sent over the Wi-Fi WAN connection rather than the cellular network. With SNF for Unreliable Mode enabled, if the Wi-Fi WAN connection is active and the cellular connection is not (i.e. out of the cellular coverage area) reports continue to be sent over Wi-Fi. Only if both networks are down are the reports stored and forwarded later when either network is back up.* *Note: You can also use an AT Command to set this value. For more information, see *PPSNF on page 427.*

Table 9-1: GPS: Servers 1 – 4

Field	Description
SNF Reliable Mode	Store and Forward Reliability: GPS reports are retransmitted if not acknowledged by the server. Options are: • OFF (Unreliable Mode) (default)—If this field is Off, the device does not expect acknowledgment to any GPS report sent to the server. • Reliable Mode—A sequence number (1–127) is added to each packet (page). The server acknowledges every 8th packet. If there is no ACK from the server, ALEOS pings the server and re-sends the packets when the server responds. If the server receives packets out of sequence, the server NAKs the first and last missed packets. ALEOS retransmits the missing packets. *Note: Reliable mode is valid only when a RAP report is select as the GPS Report Type.* • Simple Reliable Mode—ALEOS attempts to contact the server the configured number of times, after which it stops attempting to contact the server and discards messages that cannot be transmitted or received after the configured number of tries. When contacted, the server responds with the ASCII string UDPACK. For information on configuring the maximum number of retries see SNF Simple Reliable Max Retries on page 244. For information on configuring the backoff time, see SNF Simple Reliable Backoff Time (secs) on page 244.) • UDP Sequence Mode—A hex sequence number (30–7f) is prepended to the packet. The server responds with SEQACK and the sequence number. The sequence number is not stored and is re-initialized when the AirLink device is reset or power cycled. Unacknowledged packets are dropped after the configured number of retries. • TCP Listen Mode—This mode is the same as UDP Sequence Mode, except that the server initiates the connection using TCP. Use this mode if your server is behind a firewall. If you are using this mode, the AirLink device must have a mobile terminated/ Internet routable IP address. • TCP—When the AirLink device is out of coverage (no service, the link is down, etc.) reports are stored until the device can access the server. *Note: You can also use an AT Command to set this field. For more information, see *PPSNFR on page 427.*
SNF Simple Reliable Max Retries	When the AirLink device is configured to use Simple Reliable Mode, use this field to set the maximum number of retries when a report is sent and there is no response. Use the SNF Simple Reliable Backoff Time (secs) field to set the interval between retries. Options are: • Disabled • 1–255 retries (Default is 10.) You can also use an AT Command to set this value. For more information, see *PPMAXRETRIES on page 426.
SNF Simple Reliable Backoff Time (secs)	When the AirLink device is configured to use Simple Reliable Mode, use this field to set the interval for the retries. (Use the SNF Simple Reliable Max Retries field to set the maximum number of retries.) • (Default is 10.) You can also use an AT Command to set this value. For more information, see *PPSIMPLETO on page 427.

Table 9-1: GPS: Servers 1 – 4

Field	Description
Additional Data When configured, these options add additional data to RAP reports (see GPS Report Type **on page 240**) sent in response to any trigger.	
Report Odometer	Enables odometer reporting. Options are: • Disable (default) • Enable You can also use an AT Command to set this value. For more information, see *PPODOM on page 427.
Report Digital Inputs	Enables digital input reporting. Options are: • Disable (default) • Enable You can also use an AT Command to set this value. For more information, see *PPREPORTINPUTS on page 427.

Redundant Servers

When one or two redundant servers are enabled, each time a message is sent out to the main server a second identical message is sent to the redundant server(s).

The redundant servers can be running the same or different application than the primary server. The messages to the redundant server are independent of the primary server settings or state.

You can configure one or both redundant servers. The messages are sent independently to either or both.

Note: Messages are sent whether or not the server is available and do not use any reliable mode format. Receipt of a message is not acknowledged nor is any message resent. Messages to redundant servers are in UDP only.

GPS RAP Report Sequence Example

In this example:

The AirLink device is installed in a police car.

- Digital input 2 is connected to the switch that controls the siren.
- Digital input 3 is connected to the laptop docking station.

ACEmanager has the following configuration:

- Report Interval Time: 30 seconds
- Report Interval Distance: 150 meters
- Stationary Vehicle Timer: 5 minutes
- Send Stationary Vehicle Event in Seconds: 6 seconds
- Maximum Speed Event: 100 km/h
- Enable Digital Input Event: Enable

- Report Type: GPS + Date (RAP GPS report type 0x12)
- Low Power Mode: Low Voltage (See Services > Low Power on page 186.)

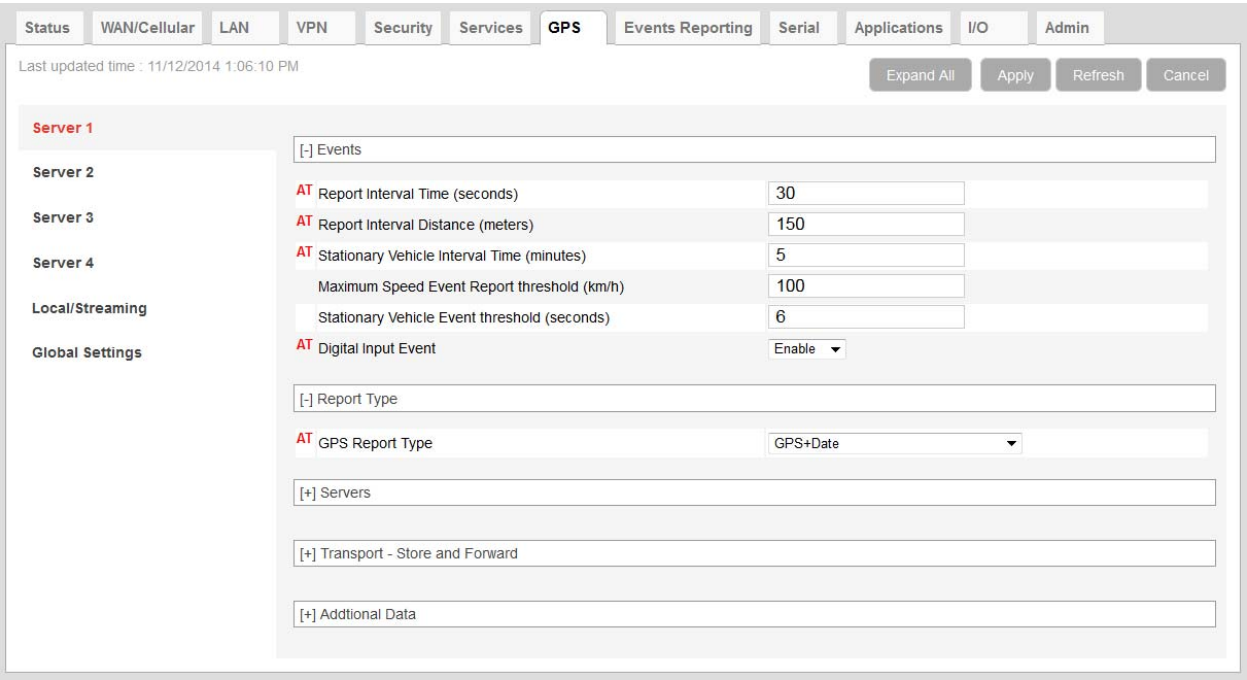


Figure 9-3: GPS > Server 1—Example

The following table provides a sample scenario for this ALEOS configuration.

Event / Action	GPS RAP report sent to the server
The AirLink device in the police car is connected to power for the first time.	A 0x10 (power up) report is sent.
The police car is driving around the patrol area.	A 0x12 (GPS + Date) report is sent every 150 meters or every 30 seconds, whichever is less.
The police officer spots a speeding vehicle, switches on the siren, and pursues the vehicle.	Digital input 2 which is connected to the siren switch is triggered and a 0x27 (DIN 2 changes to 1) report is sent.
The vehicle speeds up, with the police car in pursuit.	When the police car exceeds 100 km/h, a 0x2e (maximum speed exceeded) report is sent. A 0x12 (GPS + Date) report is sent every 150 meters.
The vehicle being pursued and the police car slow down.	When the police car's speed goes below 100 km/h, a 0x2f (return to normal speed) report is sent.
The speeding vehicle pulls over and stops at the side of the road. The police car pulls in behind it. The officer turns off the siren, leaves the engine idling, gets out of the car, and walks over to the other vehicle.	Digital input 2 which is connected to the siren switch is triggered, and a 0x26 (DIN 2 changes to 0) report is sent. Six seconds after the police car comes to a stop, a 0x2c (stationary vehicle event) report is sent. While the car remains stopped with the engine idling, a 0x12 (GPS + Date) report is sent every 5 minutes.
The officer issues a ticket, returns to the police car and drives away.	When the police car is back in motion, a 0x2d (started moving event) report is sent. A 0x12 (GPS + Date) report is sent every 150 meters or 30 seconds, whichever is less.

Event / Action	GPS RAP report sent to the server
The police car stops in front of the police station.	Six seconds after the car stops, a 0x2c (stationary vehicle event) report is sent.
The officer disconnects the laptop from the dock.	Digital input 3 connected to the docking station is triggered. A 0x28 (DIN 3 changes to 0) report is sent.
The officer turns off the ignition.	Before the AirLink device goes into Low Power (sleep) mode, it sends a 0x30 (entering low power mode) report.
The officer on the next shift gets into the car and turns on the ignition.	When the AirLink device wakes up from Low Power mode, it sends a 0x31 (Wake up from Low Power mode event) report.

Local/Streaming

Some in-vehicle/navigation applications accept GPS reports via a serial connection, generally using either NMEA or TAIP. To configure serial streaming for DB-9 (RS-232) ports and/or USB Serial ports, go to GPS > Local Streaming. If you have an AirLink GX Series device with an I/O card installed, you can also use the I/O X-Card serial ports to stream GPS data.

Note: This side tab only appear if GPS Service (on the Global Settings side tab) is Enabled.

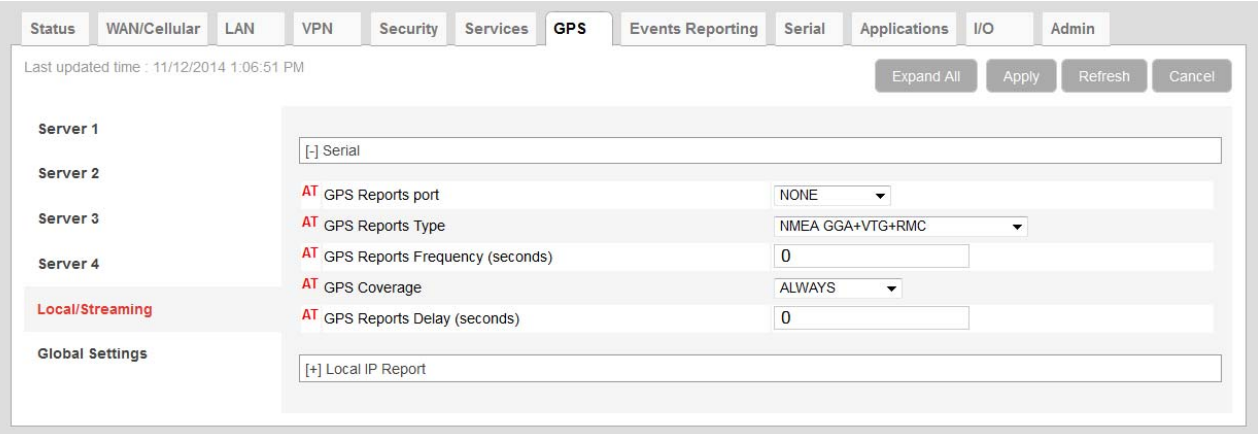


Figure 9-4: ACEmanager: GPS > Local/Streaming

Table 9-2: GPS: Local/Streaming

Field	Description
Serial	
GPS Reports port	The serial port or USB serial link that reports are sent to Options are: • NONE (default) • DB9 Serial • USB Serial • DB9 and USB • X-Card Serial • X-Card Serial and DB9 • X-Card Serial and USB • X-Card Serial, DB9 and USB You can also use an AT Command to set this value. For more information, see *PGPS on page 422. *Note: If you want to stream GPS data to a USB port, the USB port must be configured on the LAN > USB page to act as a serial port. See USB Device Mode on page 120.* *Note: The X-Card options are only available for a GX Series device with an I/O X-Card installed.*
GPS Reports Type	ASCII text GPS Report type to send via the serial link: • NMEA GGA+VTG+RMC—NMEA GPS report that contains fix information and vector track and speed over ground, and recommended minimum GPS data (default) • NMEA GGA+VTG+RMC+GSA+GSV—NMEA GPS report that contains fix information and vector track and speed over ground, the recommended minimum GPS data, overall satellite data, and detailed satellite data • TAIP data—TAIP GPS report that contains position and velocity • TAIP compact data—TAIP GPS report that contains the compact position • TAIP LN report—TAIP GPS report that contains a long navigation message • TAIP TM report—TAIP GPS report that contains the time and date You can also use an AT Command to set this value. For more information, see *PGPSR on page 423.
GPS Reports Frequency (secs)	How frequently (in seconds) the GPS report is sent to the serial link Options are: • 1–65535—(up to 18.2 hours) You can also use an AT Command to set this value. For more information, see *PGPSF on page 423. *Note: In devices with radio module MC8705, setting this field to 1 sec may result in the device providing GPS locations in intervals ranging from 1 to 3 secs (generally under 2 seconds). To determine which radio module your device has, in ACEmanager go to Status > About and check the Radio Module Type field.*

Table 9-2: GPS: Local/Streaming

Field	Description
GPS Coverage	This field refers to the cellular network coverage. Options are: • ALWAYS (default)—GPS reports are always streamed to the serial link. • Out of Coverage—GPS reports are only streamed to the serial link when the device has no cellular connection. You can also use an AT Command to set this value. For more information, see *PGPSC on page 422. **Tip:** *The Out of Coverage option enables you to use a back-up in-vehicle mapping application that does not rely on cellular network access.*
GPS Reports Delay (secs)	The delay (in seconds) before the out of the coverage stream begins. This field only applies if the GPS coverage field is set to “Out of Coverage”. • 0 (default) • 1–255 You can also use an AT Command to set this value. For more information, see *PGPSD on page 423.

Local/Streaming—Local IP Report

Local IP reports are limited to tethered IP-based LAN hosts (Ethernet, USB/net, DUN, PPPoE). Local IP reports do not have any transport/SNF options. The reports are always sent regardless of cellular coverage.

The destination IP cannot be configured directly. The first connected LAN host is used. If multiple hosts are connected, the priority is the host using the Public IP address, or if all hosts are using Private IP addresses, the priority is:

- Ethernet
- USB
- DUN

Note: This side tab only appear if GPS Service (on the Global Settings side tab) is Enabled.

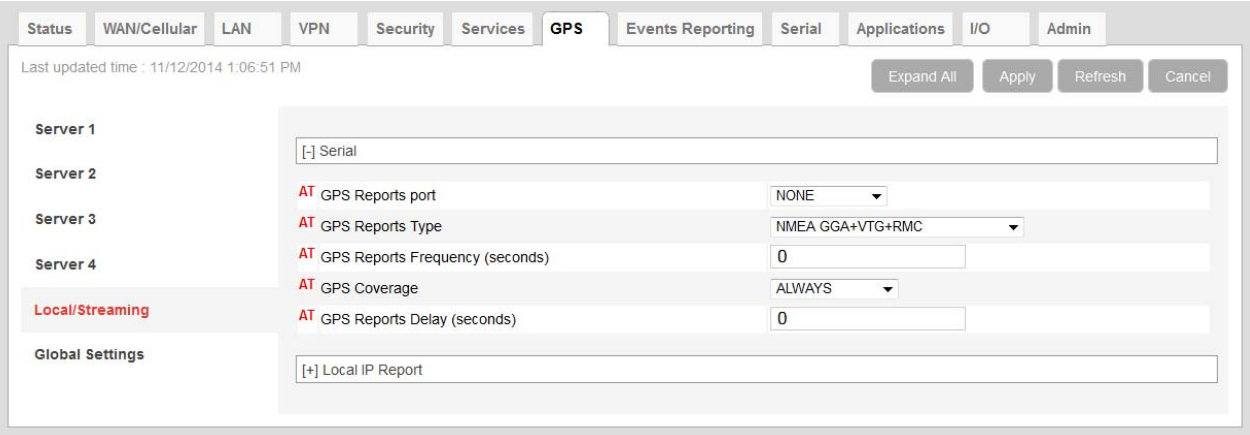


Figure 9-5: ACEmanager: GPS > Local/Streaming: Local IP report

Table 9-3: GPS: Local/Streaming—Local IP Report

Field	Description
Local Reporting Time Interval (Secs)	The frequency (in seconds) of the reports Options are: • 0 = Disable (default) • 1–255 You can also use an AT Command to set this value. For more information, see *PPLATS on page 425. *Note: If the Local Reporting Time Interval is set to 1 second, there may be some variation in the report interval, with the report interval sometimes being less than 1 second and sometimes more than 1 second. Other settings for this field are accurate.*

Table 9-3: GPS: Local/Streaming—Local IP Report

Field	Description
Local Report Type	Sets one of the following Local Report types: RAP • GPS Data—RAP GPS report that contains only GPS data • GPS+Date—RAP GPS report that contains GPS data with the UTC time and date (default) • GPS+Date+RF—RAP GPS report that contains GPS data, the UTC time and date, and radio frequency information for the cellular connection • GPS+Date+RF+EIO—RAP GPS report that contains GPS data, the UTC time and date, radio frequency information for the cellular connection, and the current I/O state NMEA • NMEA GGA+VTG—NMEA GPS report that contains fix information, vector track, and speed over ground • NMEA GGA+VTG+RMC—NMEA GPS report that contains fix information, vector track, speed over ground, and recommended minimum GPS data • NMEA GGA+VTG+RMC+GSA+GSV—NMEA GPS report that contains fix information, vector track, speed over ground, the recommended minimum GPS data, overall satellite data, and detailed satellite data TAIP • TAIP data—TAIP GPS report that contains position and velocity • Compact TAIP data—TAIP GPS report that contains the compact position • TAIP LN report—TAIP GPS report that contains a long navigation message • TAIP TM report—TAIP GPS report that contains the time and date. *Note: You can also use an AT Command to set this value. For more information, see *PPLATSR on page 426.* *Note: Local IP Report does not have an option for Xora reports.*
Starting Destination Port	The primary port that reports are sent to The Local IP report source port is 17335. This is not configurable.
Number of Extra Destination Ports	You can send the report to up to 7 additional consecutive ports. For example, if the starting port is 12351 and you set this field to 5, reports are sent to ports 12351, 12352, 12353, 12354, 12355, and 12356. The default is 0 which means only the starting port is used. You can also use an AT Command to set this value. For more information, see *PPLATSEXTRA on page 426.

Table 9-3: GPS: Local/Streaming—Local IP Report

Field	Description
Device ID in Local Reports	Allows use of the IMEI/ESN or phone number in local IP RAP reports to identify a device/vehicle. Options are: • None (default) • Phone Number • ESN/IMEI **Tip:** *Including the device ID is especially useful when your devices have dynamic IP addresses.* *Note: If you want the device ID included in all other RAP GPS reports, see Use Device ID in Location Reports on page 254.*
Local Report Destination IP	This read-only field shows the IP address of the destination that Local IP reports are send to. Through its use of DHCP, ALEOS detects if there is a connected host and designates that host's IP as the local IP destination. When no host is connected at startup, ALEOS uses the first IP address in the Ethernet DHCP pool as the destination. When using Public mode for an interface, that interface will be the local IP destination even if it's not the first host connected. *Note: The Local Report Destination IP is not configurable. If you want a GPS report to go to a specific host IP, user Server 1–4 configuration. (See Servers 1 to 4 on page 235.)*
Report Odometer	Enables odometer reporting Options are: • Disable (default) • Enable *Note: Only applies for RAP report types.*
Report Digital Inputs	Enables digital input reporting. Options are: • Disable (default) • Enable *Note: Only applies for RAP report types.*

Global Settings

Most of the Global settings apply to all GPS Server and Local reports.

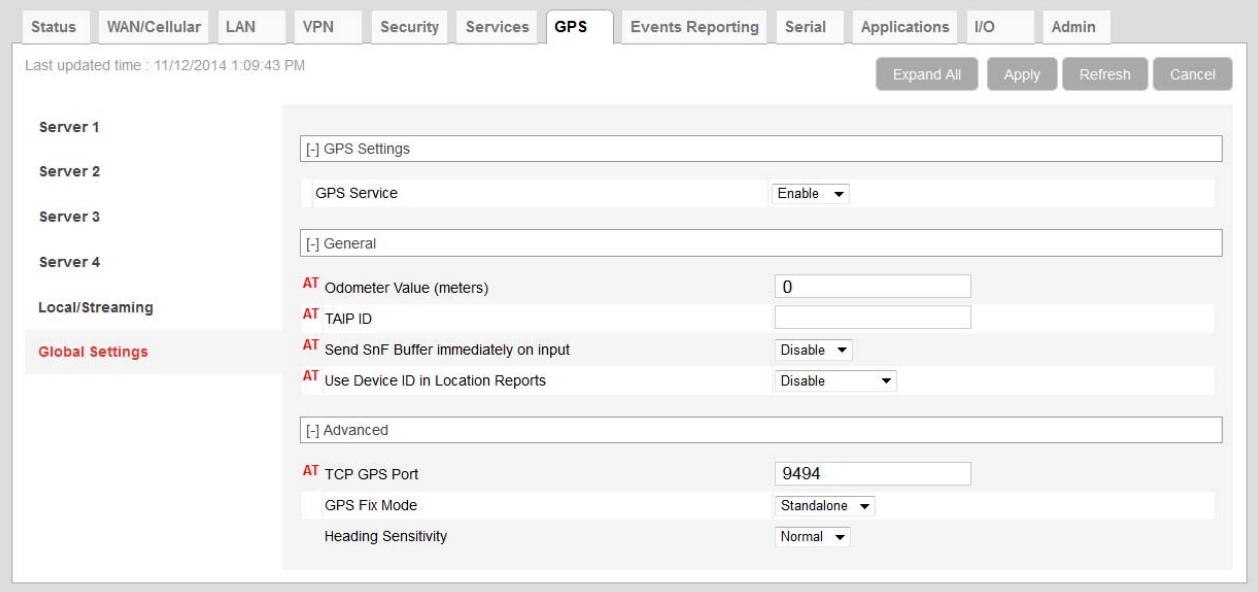


Figure 9-6: ACEmanager: GPS > Global Settings

Table 9-4: GPS: Global Settings

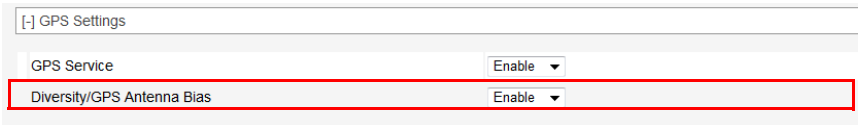
Field	Description
GPS Settings	
GPS Service	Sierra Wireless recommends that you disable GPS if you are not using GPS reporting. Options are: • Enable (default) • Disable
Diversity/GPS Antenna Bias	This field applies only to the LS300, and only appears if GPS Service is enabled.  Configure this field according to the type of GPS antenna you are using. Check the antenna manufacturer's documentation to determine if you have an active or passive GPS antenna. Options are: • Enable (default)—Use the default setting if you are using an amplified (active) GPS antenna. • Disable—Disable this feature if you are using a passive GPS antenna. *Note: If GPS Service is disabled, antenna bias is automatically disabled.*

Table 9-4: GPS: Global Settings (Continued)

Field	Description
General — These fields only appear is GPS Service is enabled.	
Odometer Value (meters)	The odometer value increments based on the GPS distance traveled. You can include this value in RAP GPS reports. (See GPS Report Type on page 240). You can set the odometer value to an initial value. Maximum value is 4 294 967 295 meters (4,294,967 kilometers or 2,668,769 miles). Default: 0 *Note: The RAP report displays the odometer value in 100s of meters.* You can also use an AT Command to set this value. For more information, see *PPODOMVAL on page 427.
TAIP ID	The four character alphanumeric ID used in all TAIP reports You can also use an AT Command to set this value. For more information, see *PPTAIPID on page 428.
Send SnF Buffer immediately on input	If this feature is enabled, any pending stored reports are sent if the I/O input changes, a stationary vehicle is moved, or a maximum speed is exceeded, provided those events are enabled on the GPS > Server > Events screen. Options are: • Disable (default) • Enable You can also use an AT Command to set this value. For more information, see *PPFLUSHONEVT on page 424.
Use Device ID in Location Reports	Allows use of the IMEI/ESN or phone number in RAP reports configured for Servers 1–4 to identify a device/vehicle. Options are: • None (default) • Phone Number • ESN/IMEI You can also use an AT Command to set this value. For more information, see *PPDEVID on page 424. **Tip:** *Including the device ID is especially useful when your devices have dynamic IP addresses.* *Note: The device ID in RAP reports is in hex, not plain text.* *Note: This option does not apply to Local IP reports. If you want the device ID included in local IP GPS reports, see Device ID in Local Reports on page 252.* *Note: If you want this Device ID included in the TCP PAD connections, enable the Include Device ID on TCP Connect field on the Serial screen (Serial > Port Configuration > TCP). See Port Configuration on page 275.*

Table 9-4: GPS: Global Settings (Continued)

Field	Description
Advanced—These fields only appear is GPS Service is enabled.	
TCP GPS Port	You can obtain a single location snapshot from the device via a TCP session using the AirLink device's IP address and the device port configured in this field. • 1–65535 (default 9494) • 0 = Disable You can also use an AT Command to set this value. For more information, see *PPTCPPOLL on page 428. *Note: Access is restricted to the IP address defined for server 1. (See Report Server IP Address on page 241.)*
GPS Fix Mode	Specifies the GPS fix mode. Options are: • Standalone (default) • MS Based—(Mobile Station Based fix) Uses assistance GPS data from a remote server over the WAN interface
Heading Sensitivity	Sets the sensitivity of the GPS heading reading • Normal (default) • High It is recommended that you leave the field set to Normal to avoid showing misleading heading values from poor GPS signal (poor sky view, reflections in urban canyon, etc.), but if your GPS application has its own GPS heading sensitivity algorithms, try changing this setting to High.

10: Events Reporting Configuration

10

Introduction

Events Reporting allows you to generate reports or perform actions in response to the events that are configured in the ALEOS software.

An Event is a measurement of a physical property AND a state change or a threshold crossing. For example, radio module signal strength (RSSI) is a physical property. A threshold crossing could be set to -105 dBm. You can configure an Event which consists of the RSSI with the -105 dBm threshold. There are many Events that can be configured; these are described in detail below.

An Action is an activity which can be performed, such as sending a report to a remote server, sending an email or an SNMP trap, changing the value on a digital signal line, or turning off cellular communication with any devices connected to a host port. For email and some other reports, you can select the data to be included.

Events and Actions work together. When an Event occurs (such the state of a monitored physical property changing or a threshold being crossed), it triggers the configured Action. For example, if you have configured an RSSI Event, you can have a report (such as an email, SNMP trap, or SMS Message) sent when the threshold is crossed. This relationship is shown conceptually in Figure 10-1.

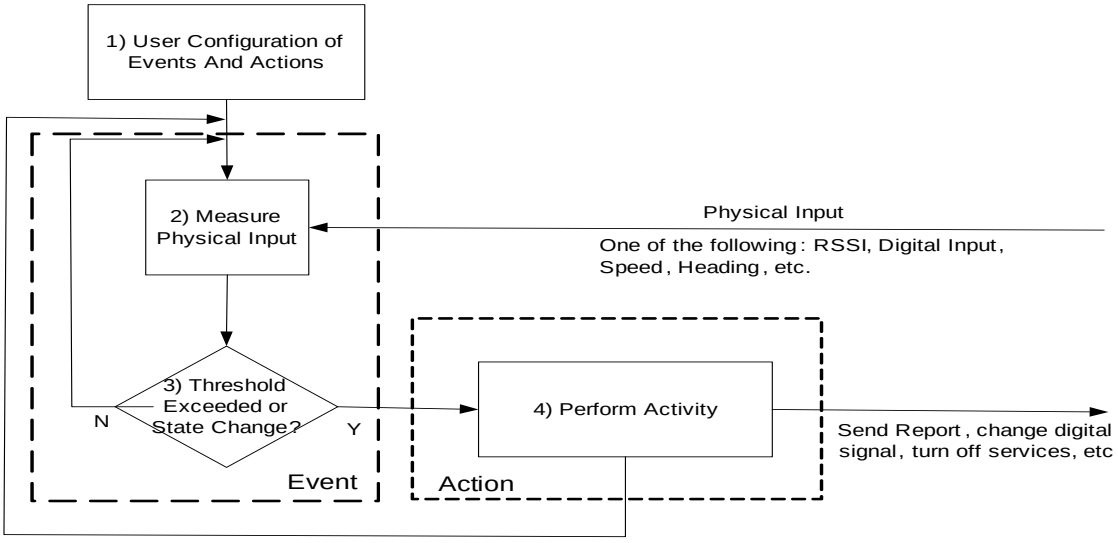

1) User Configuration of Events And Actions
2) Measure Physical Input
Physical Input
One of the following: RSSI, Digital Input, Speed, Heading, etc.
3) Threshold Exceeded or State Change?
N
Y
Event
4) Perform Activity
Action
Send Report, change digital signal, turn off services, etc

Figure 10-1: Events Reporting Concept

The process works as follows:

1. Configure the events and actions.
2. After deployment, the device begins measuring a physical input.

3. The measurement is compared to the configured threshold or state change. If there is no change, then another measurement is performed. If a state change (or threshold crossing) occurs, then the flow moves to step 4.
4. The Action associated with the Event in this step occurs. A report may be generated or some other activity is performed. Afterwards, the flow returns to step 1.

Additional Behavior and Features

Events/Actions are not one shot activities. After an Action is performed, the Event is still active and will trigger the next time the state change or threshold crossing occurs.

A single Event may activate one or more Actions. For example, if RSSI is below threshold, you can send an email (Action 1) and send an SMS message (Action 2).

A single Action may be activated by one or more Events. For example, if network state changes to Network Ready, or the RSSI crosses a configured threshold, either Event can perform the same action.

After defining an Event, always select the Apply button to save these definitions and apply them to an Action.

Selecting the Delete button on the Events Reporting tab will delete all current Event and Action data.

Configuring Events Reporting

When configuring Events Reporting, first configure the event you want reported. Then configure the Action (that is, how you want to be notified when the event occurs), and finally, link the Event to the Action.

Note: All Events Reporting configuration changes take effect after a short delay (about one minute). No reboot of the AirLink device is necessary.

To configure Events and Actions:

1. In ACEmanager, go to Events Reporting.
2. Select Actions from the menu on the left of the screen.

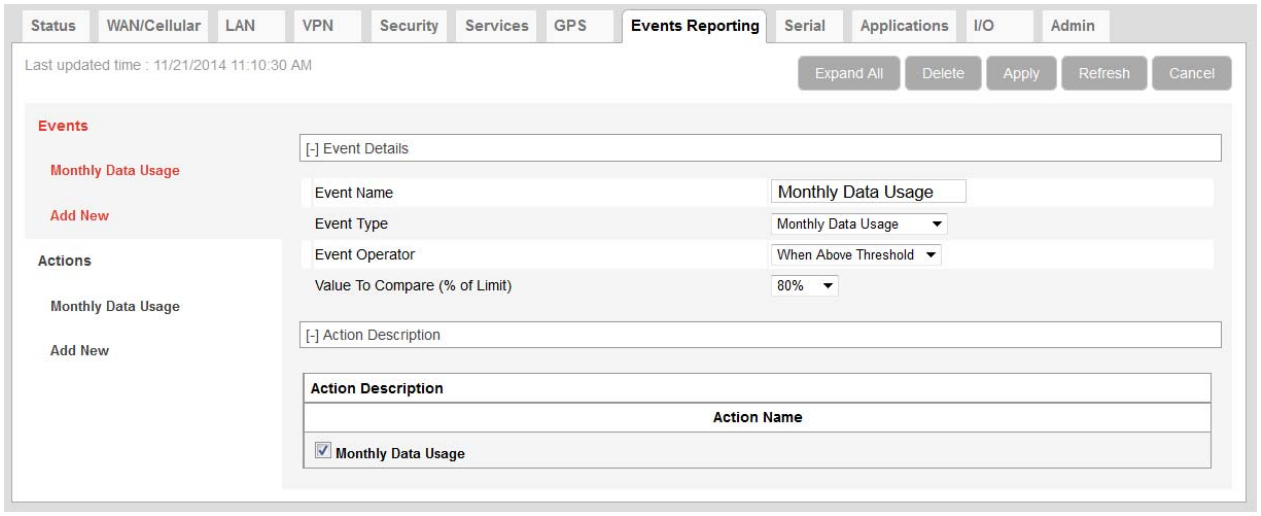


Figure 10-2: ACEmanager: Events Reporting > Actions

3. Define an Action:
   a. Enter a name for the action.
   b. Select the Action Type. For more information, see Action Types on page 260.
   c. Enter the parameters.

      The parameters vary depending on the Action Type choose. For a complete list of Actions and additional information, see Action Types on page 260.
4. Click Apply.
5. Select Events from the menu on the left.

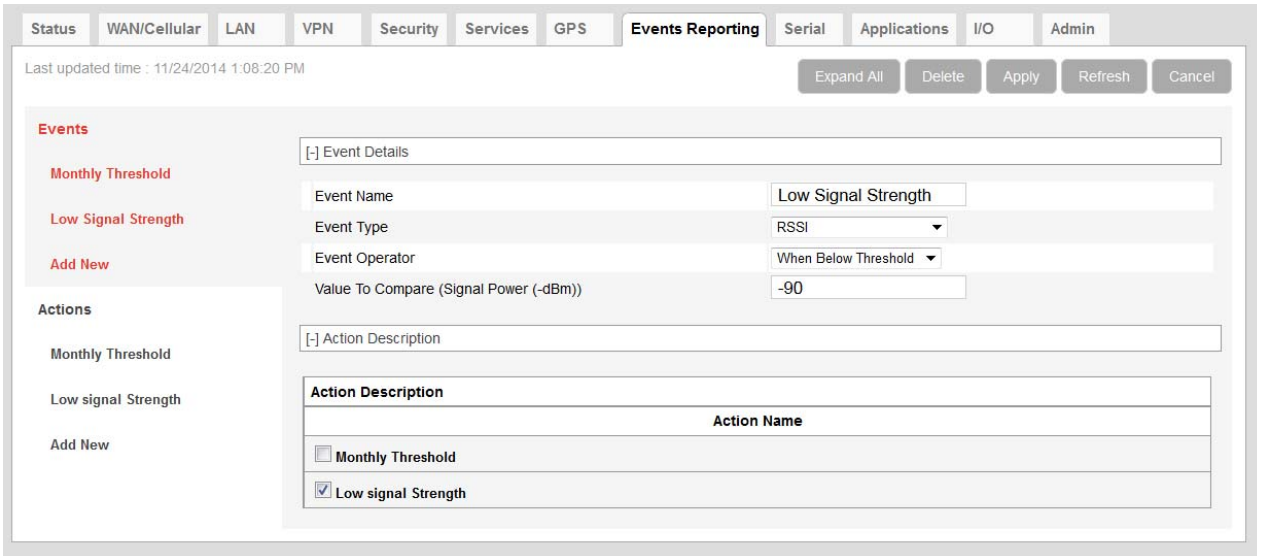


Figure 10-3: ACEmanager: Events Reporting > Events

6. Define an Event:
   a. Enter a name for the event.

b. Select the Event Type. For more information, see Event Types on page 271.

c. Select the Event Operator and choose the parameters.

   The parameters vary depending on the Event Type and Event Operator chosen. For more information, see Table 10-1 on page 271.

7. Associate the Action with the Event:

   a. Under Action Description, select the check box beside the name of the action you want to associate with the new event.

8. Click Apply.

Action Types

Note: You can define a maximum of 5 Actions.

If an Action requires an IP connection, the following source ports are used. These are not configurable.

Actions (in the order configured)	Source port
Action 1	17348
Action 2	17349
Action 3	17351
Action 4	17352
Action 5	17353

Note: If you select Email or SNMP TRAP as the Action Type, be sure that these options are configured on the Services tab. Go to Services > Email (SMTP) or Services > Management (SNMP).

Under the Events Reporting Action tab, the Action Type drop-down menu shows the Action Types available for the device you are configuring.

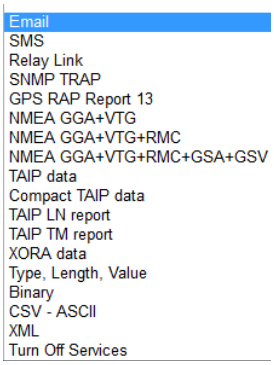


Figure 10-4: *ACEmanager: Events Reporting > Action > Action Type drop-down menu*

There are several ways to send a report. The configuration varies.

Email

- **To** — The email address where the report should be sent.
- **Subject** — The subject that should be displayed.
- **Message** — The message you want included with each report.
- **Body Type** — Select message in ASCI Text, SVS SCI and XML.
- **Test report** — Use to send a test report. After you have updated all the fields and clicked the Apply button, wait about 1 minute, and then click the Test report button.

Note: If you are using Email as the Action for an Event, you must also configure the email server settings on the Services > Email (SMTP) tab and reboot the device. See Email (SMTP) on page 218.

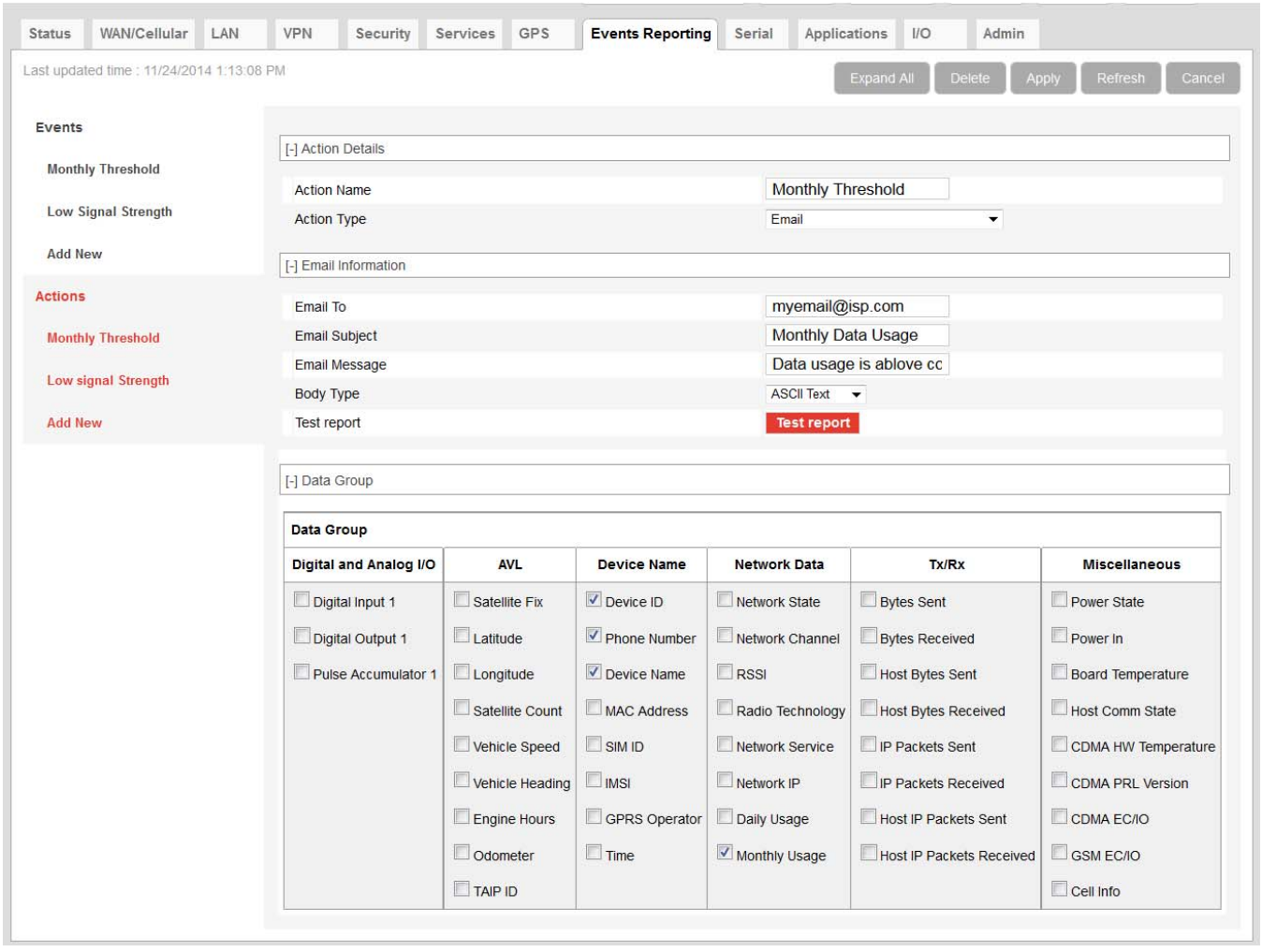


Figure 10-5: ACEmanager: Events Reporting > Action Type > Email

Note: If you are using this option, be sure Email is configured on the Services > Email (SMTP) tab. For more information, see Email (SMTP) on page 218.

SMS text message

- **To** — The email address where the report should be sent.
- **Subject** — The subject that should be displayed.
- **Message** — The message you want included with each report.
- **Body Type** — Select message in ASCI Text, SVS SCI and XML.
- **Test report** — Use to send a test report. After you have updated all the fields and clicked the Apply button, wait about 1 minute, and then click the Test report button.

Note: You can only send SMS from your AirLink device if your cellular account allows SMS. You may need to have SMS added to the account. SMS from data accounts is blocked on some cellular networks.

Note: Outgoing SMS messages are limited to 140 characters. If the selected data exceeds 140 characters, the message is truncated (and contains a note indicating that it has been truncated.

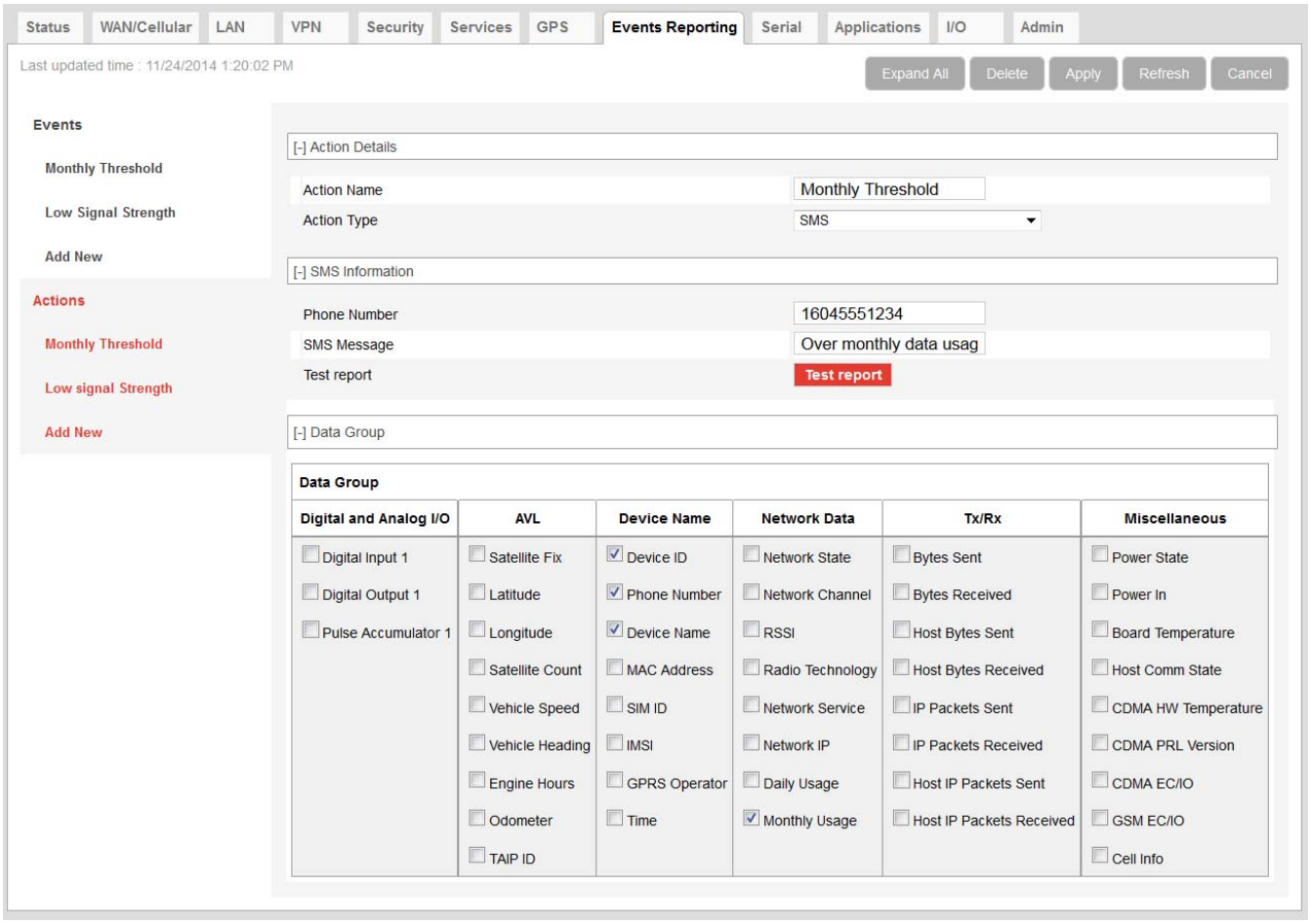
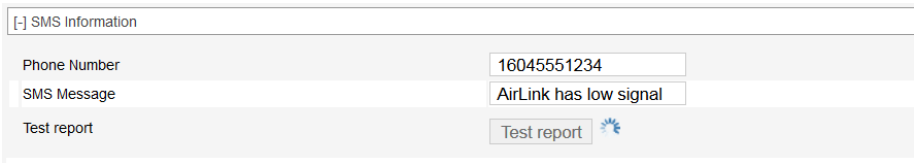


Figure 10-6: *ACEmanager: Events Reporting > Action Type > SMS*

To send a test SMS:

1. Enter the desired phone number and SMS message.
2. Click Apply.
3. Wait until the progress circle disappears and the Test report button is enabled.



4. Once it is enabled, click the Test report button to send a test SMS.

SNMP Trap notification

Note: If you are using this option, be sure SNMP Trap is configured on the Services > Management (SNMP) page.

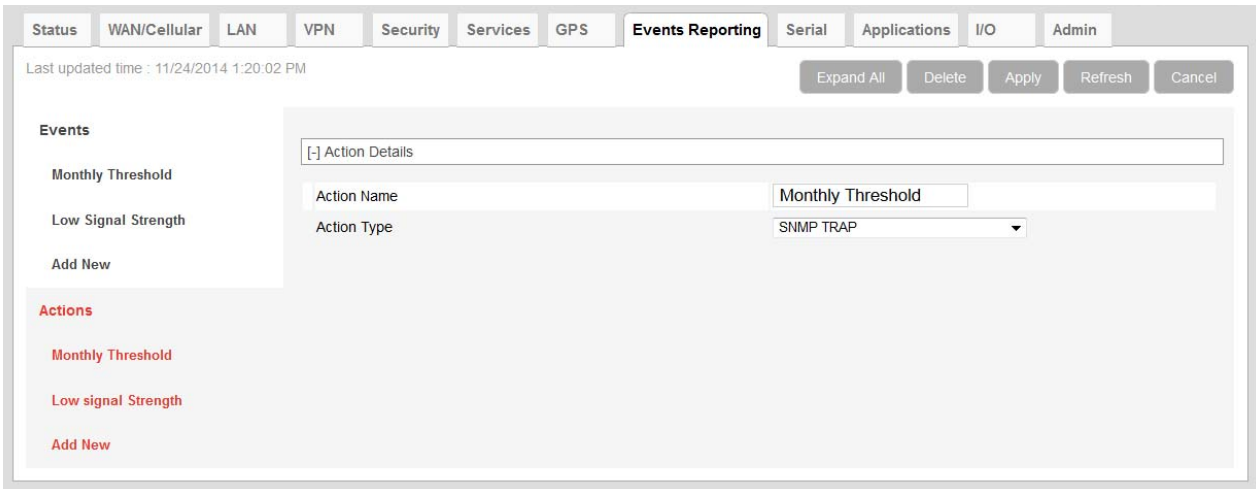


Figure 10-7: ACEmanager: Events Reporting > Action Type > SNMP TRAP

Relay Link

- Select the relay to link to, and invert if necessary.

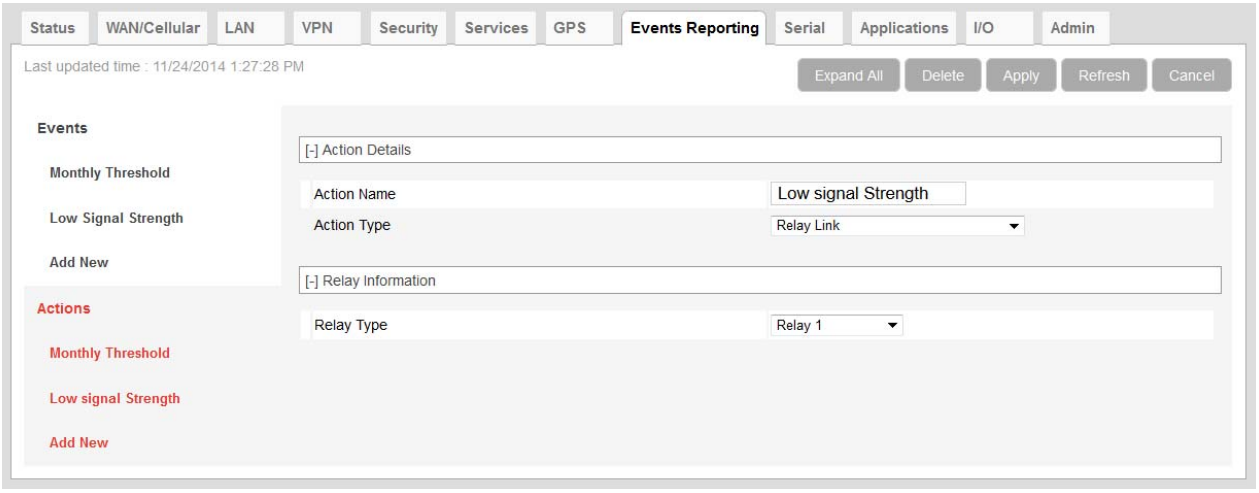


Figure 10-8: ACEmanager: Events Reporting > Action Type > Relay Link

GPS RAP Report 13 message

- Configure the report server store and forward properties and report options.

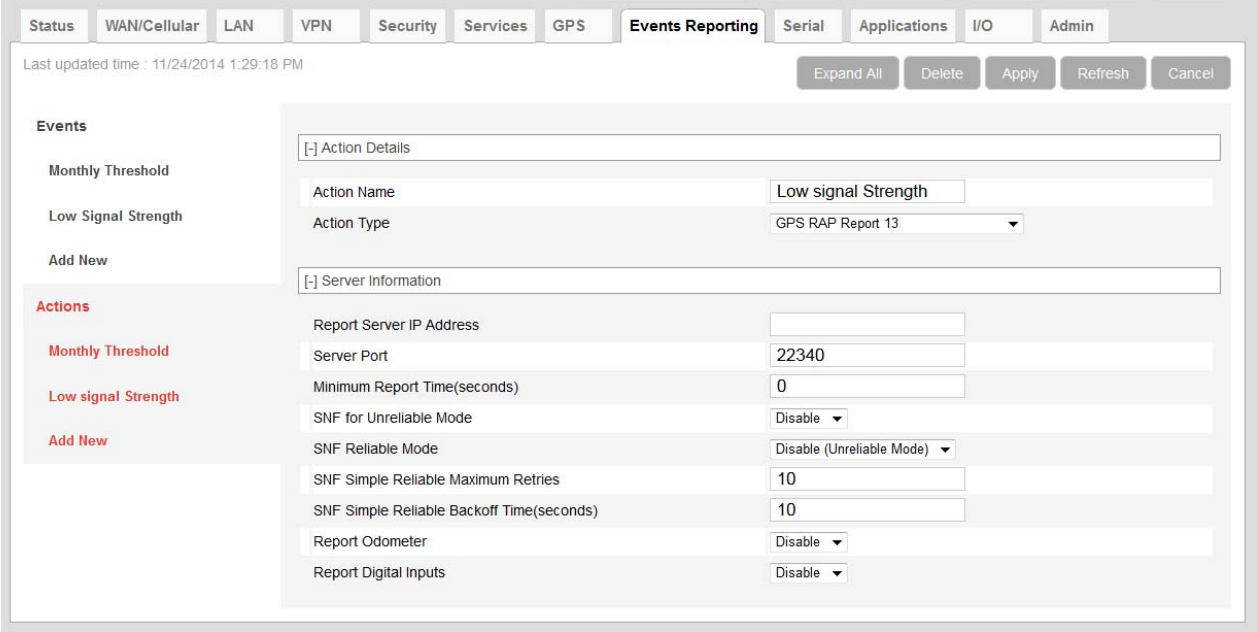


Figure 10-9: ACEmanager: Events Reporting > Action Type > GPS RAP Report 13

Events Protocol message to a server

The Events Reporting protocol is a collection of messaging formats. The messages are sent to the configured Reports Server.

The Events Protocol includes four message types.

- **1 — Type, Length, Value** — The TLV consists of the MSCI ID as the type, the length of the data, and the actual data.
- **2 — Binary** — A binary condensed form of the TLV message is sent.
- **3 — CSV-ASCII** — An ASCII condensed and comma delimited form of the TLV message is sent.
- **4 — XML** — An XML form of the data is sent.

Tip: *Because of its flexibility and robustness, the TLV message type is recommended for most reports using the Events Protocol. The Binary and ASCII forms do not contain a "type field" which can result in misinterpretation of data. Since the TLV and XML forms always include the type as well as the data, an unintentional type can be identified much easier.*

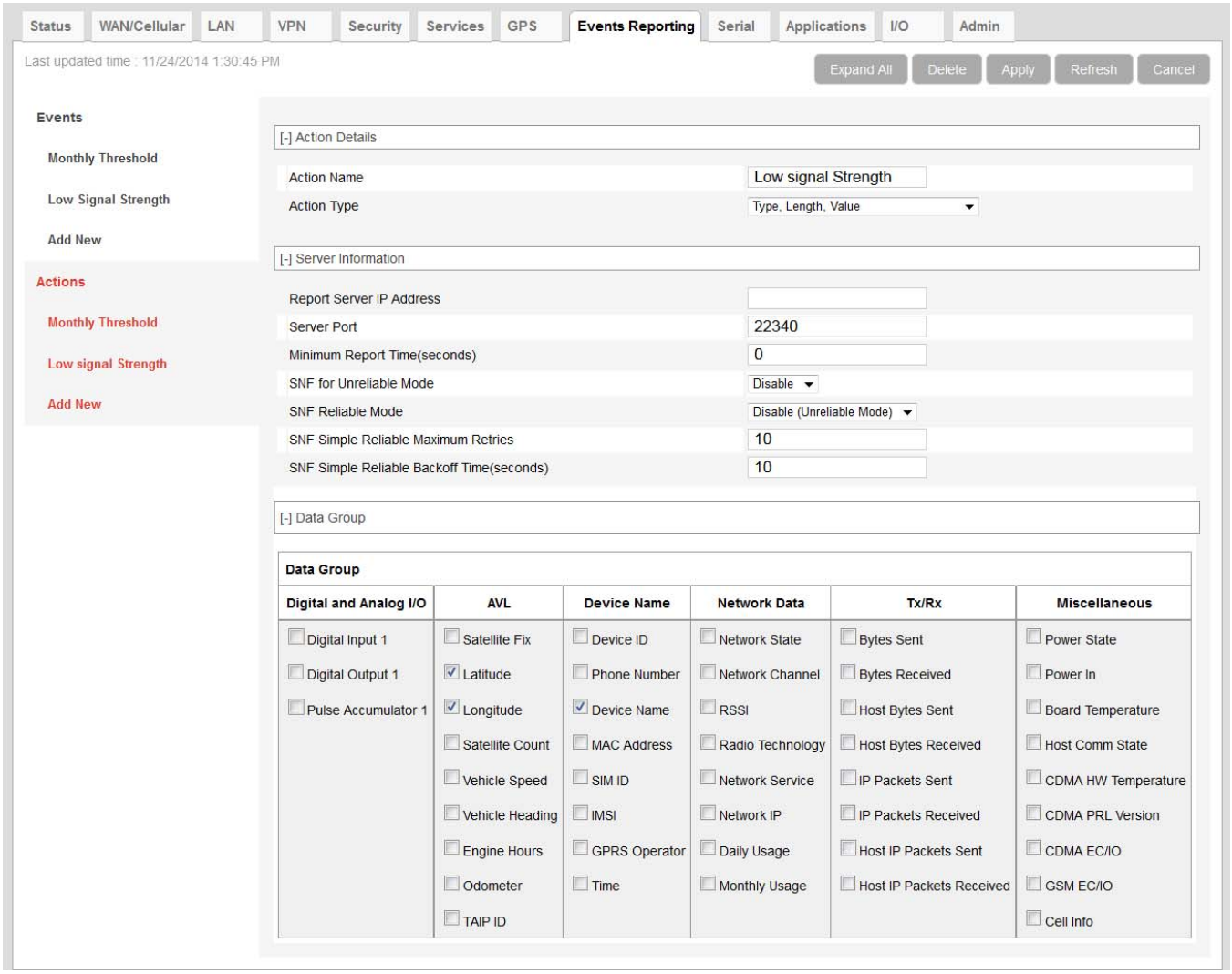


Figure 10-10: ACEmanager: Events Reporting > Action Type > Type, Length, Value

Turn Off Services

This setting limits services and is primarily used in conjunction with monitoring data usage. For example, you could set the AirLink device to limit network service when data usage exceeds a configured threshold. For more information, see Data Usage on page 303.

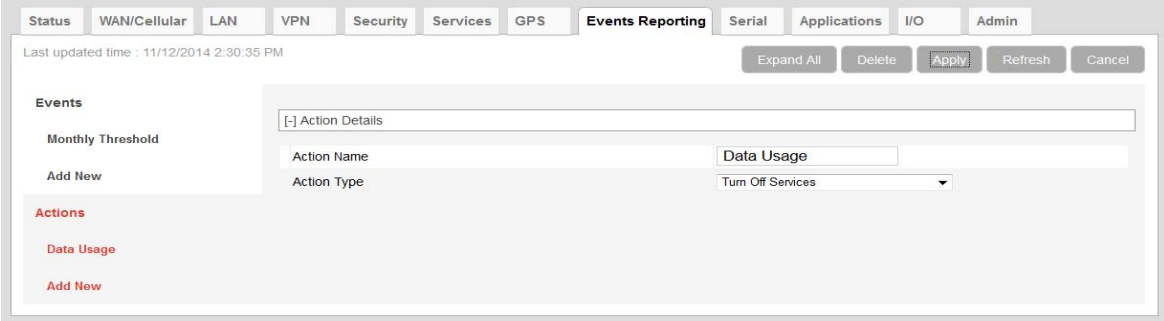


Figure 10-11: ACEmanager: Events > Actions > Action Type > Turn Off Services

Turn Off Services does not turn off all network use. Reports are still sent and over-the-air access to the device is allowed. You can still access the AirLink device locally, but Ethernet, USBnet, and Wi-Fi access to the Cellular network is blocked.

Report Data Group

For email, SMS, and Events Protocol (TLV, Binary, CSV-ASCII, and XML) messages, you can select the data you want to be included in the report. Check the box corresponding to the data displayed. By default, all the boxes are clear.

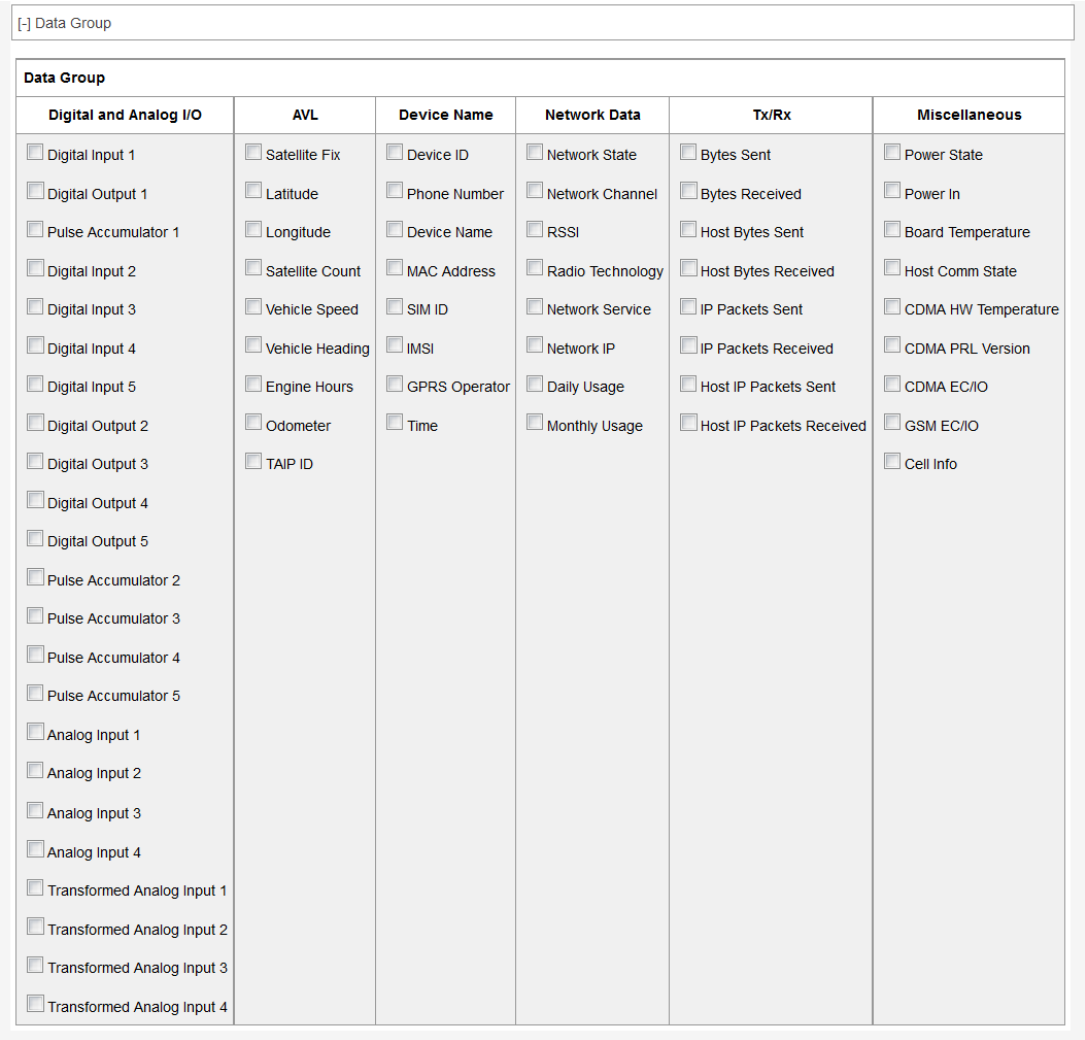


Figure 10-12: *ACEmanager: Events Reporting > Action (for GX device with I/O X-Card installed)*

The reports attributes are:

- Digital and Analog I/O

  The options available in this section depend on the AirLink device, and in the case of the AirLink GX Series device, whether or not it has an I/O X-Card installed.

  - Include Digital Inputs 1–5—The status of the specific digital inputs
  - Include Digital Outputs 1–5—The status of the specific digital outputs
  - Include Pulse Accumulator 1–5—The pulse count of the specific digital inputs
  - Include Analog Inputs 1–5— The status of the specific analog input (reported in volts)
  - Include Transformed Analog Inputs 1–5— The status of the specific analog input (reported in units configured in ACEmanager I/O > Configuration—see Configuration on page 321)

- AVL
  - Include Satellite Fix—Whether or not there is a usable GPS satellite fix
  - Include Latitude—The latitude reported by GPS
  - Include Longitude—The longitude reported by GPS
  - Include Satellite Count—The number of satellites the GPS is using to get a satellite fix
  - Include Vehicle Speed—The speed of the vehicle reported by GPS
  - Include Vehicle Heading—The direction the vehicle is traveling reported by GPS
  - Include Engine Hours—The number of hours the engine has been on, based on either Power In or Ignition Sense
  - Include Odometer—The number of miles reported by GPS
  - Include TAIP ID—The TAIP ID for the AirLink device
- Device Name

  These elements in the Device Name group are general identifiers for the AirLink device and its cellular account.
  - Include Device ID—The device ID (ESN or EID/IMEI) of the AirLink device (Include a cellular account with a dynamic IP address)
  - Include Phone Number—The phone number of the AirLink device
  - Include Device Name—The name of the AirLink device
  - Include MAC Address—The MAC Address of the Ethernet port of the AirLink device
  - Include SIM ID—The SIM ID of the AirLink device
  - Include IMSI—The IMSI of the SIM installed in the AirLink device
  - Include GPRS Operator—The wireless Mobile Network Operator the SIM card is associated with
  - Include Time—The time the AirLink device is active
- Network Data

  The Network Data in this group relates to the cellular network and the connection state of the AirLink device.
  - Include Network State—The network state for the AirLink device
  - Include Network Channel—The network channel to which the AirLink device is connected
  - Include RSSI—The signal strength for the AirLink device
  - Include Network Service—The network service for the AirLink device
  - Include Network IP—The IP address given by the cellular network
  - Include Daily Usage —The daily usage of the AirLink device (Units as configured on the Applications > Data Usage screen)
  - Include Monthly Usage —The monthly usage of the AirLink device (Units as configured on the Applications > Data Usage screen)
- Tx/Rx

  The Network Traffic in this group relates to the cellular network and the network between the AirLink device and any directly connected device(s).
  - Include Bytes Sent—The number of bytes sent on the cellular network since last reset
  - Include Bytes Received—The number of bytes received from the cellular network since last reset

  - Include Host Bytes Sent—The number of bytes sent from the network between the AirLink device and the connected device(s) since last reset
  - Include Host Bytes Received—The number of bytes received from the network between the AirLink device and the connected device(s) since last reset
  - Include IP Packets Sent—The number of IP packets sent on the cellular network since last reset
  - Include IP Packets Received—The number of IP packets received from the cellular network since last reset
  - Include Host IP Packets Sent—The number of IP packets sent from the network between the AirLink device and the connected device(s) since last reset
  - Include Host IP Packets Received—The number of IP packets received from the network between the AirLink device and the connected device(s) since last reset
- Misc Data

  Miscellaneous Data includes temperature rates and other information that does not fit in the other categories
  - Include Power In—The voltage level of the power coming in to the AirLink device at the time of the report
  - Include Board Temperature—The temperature of the internal hardware of the AirLink device at the time of the report
  - Include Host Comm State—The signal level between the AirLink device and the connected device(s)
  - CDMA HW Temperature—The temperature of the internal radio module
  - CDMA PRL Version—PRL version used by the AirLink device
  - CDMA EC/IO—The quality of the signal from the cellular CDMA network
  - GSM EC/IO—The quality of the signal from the cellular GSM network
  - Cell Info—The cellular network cell information for the AirLink device

Relay

The relay outputs on the AirLink device I/O port can be used to cause an external action.

- 1—Relay 1—Open
- 2—Relay 1, Inverted—Closed

The relays are capable of switching small loads. If you need a stronger signal, such as to open a door lock, connect the AirLink device's relay to a stronger solenoid relay that has enough power to cause the desired effect.

Event Types

Note: You can define a maximum of 5 events.

Table 10-1: Event Types

Event Name	Event Type	Event Operator Options	Values to Compare
Digital Inputs			
Digital Input The AirLink LS300 has 1 digital input. The AirLink GX Series device without an I/O X-Card has 1 digital input. If the GX device has an I/O X-Card installed, 4 additional digital inputs are available.	State Change	• Disable • When Switch Closed • When Switch Opened • On any change	N/A
Pulse Accumulator The AirLink LS300 has 1 pulse accumulator. The AirLink GX Series device without an I/O X-Card has 1 pulse accumulator. If the GX device has an I/O X-Card installed, 4 additional pulse accumulators are available.	Threshold Crossing	• Disable • When Changed By	• Pulse Accumulator Delta • Starting Trigger Value
Analog Input (volts) The AirLink LS300 has 1 analog input. The AirLink GX Series device with an I/O X-Card installed has 5 analog inputs available.	Threshold Crossing	• Disable • When Above Threshold • When Below Threshold • When Cross Threshold	Value To Compare (Threshold (volts))
Transformed Analog AirLink LS300 has 1 transformed analog input. The AirLink GX Series device with an I/O X-Card installed has 5 transformed analog inputs available.	Threshold Crossing	• Disable • When Above Threshold • When Below Threshold • When Cross Threshold	Value To Compare (Units configured on the I/O screen) See Transformed Analog on page 322.

Note: Analog Input 1 and Transformed Analog Input 1 are only available on the LS300. Additional options are available on a GX device with an I/O X-Card installed (see Figure 10-12 on page 268).

Table 10-1: Event Types (Continued)

AVL			
GPS Fix	State Change	• Disable • Fix Lost • Fix Obtained • On any change	N/A
Vehicle Speed	Threshold Crossing	• Disable • When Above Threshold • When Below Threshold • When Cross Threshold	Value To Compare (Vehicle Speed (KM/h))
Heading Change	Threshold Crossing	• Disable • Change in Direction	Value To Compare (Heading Change (degrees))
Engine Hours	Threshold Crossing	• Disable • When Changed By	Value To Compare (Engine Hours)
Network			
RSSI	Threshold Crossing	• Disable • When Above Threshold • When Below Threshold • When Cross Threshold	Value To Compare (Signal Power (-dBm))
Network State	State Change	• Disable • When Cellular is Ready (Triggered when a cellular connection is established) • When Wi-Fi is Ready (Triggered when a Wi-Fi connection is established) • When either is Ready (Triggered when either a cellular or Wi-Fi connection is established) *Note: The last two options require a GX Series device with a Wi-Fi X-Card installed.*	N/A
Network Service	State Change	• Disable • On Service • On No Service • On Change	Value To Compare (Network Service): • Roaming • 2G Service • Rev A or HSUPA • Any Data Service
Other Report Types			
Periodic Reports	Threshold Crossing (Time)	• Disable • Periodically	Value To Compare: Report Period (secs)

Table 10-1: Event Types (Continued)

Power In	Threshold Crossing	• Disable • When Above Threshold • When Below Threshold • When Cross Threshold	Value To Compare (Power In Threshold (volts))
Board Temperature	Threshold Crossing	• Disable • When Above Threshold • When Below Threshold • When Cross Threshold	Value To Compare (Temperature Threshold (°C))
CDMA HW Temperature	Threshold Crossing	• Disable • When Above Threshold • When Below Threshold • When Cross Threshold	Value To Compare (Temperature Threshold (°C))
Data Usage			
Daily Data Usage	Threshold Crossing	• Disable • When Above Threshold	Value To Compare (% of Limit)
Monthly Data Usage	Threshold Crossing	• Disable • When Above Threshold	Value To Compare (% of Limit)

Note: You can only configure one event with either a Daily Data Usage or Monthly Data Usage trigger. If you configure more than one, for example, a trigger when the Daily Data Usage reaches a certain percentage and a trigger when the Monthly Data Usage reaches a certain percentage, only the last threshold configured is used.

ALEOS Data Usage is approximate and should not be compared with data usage recorded by the Mobile Network Operator. SIERRA WIRELESS IS NOT RESPONSIBLE FOR DATA OVERAGES.

11: Serial Configuration

11

Use the serial port to connect devices or computers using a DB9-RS232 connection.

Note: These commands are specific to the RS232 port and generally do not apply to USB/serial.

Port Configuration

Serial Port Configuration consists of five categories of configurable parameters:

- Port Configuration
- Advanced
- TCP
- UDP
- PPP

These categories and their parameters are shown in Figure 11-1, Figure 11-2, and Figure 11-3 and described in Table 11-1, Table 11-2, and Table 11-3.

Port Configuration

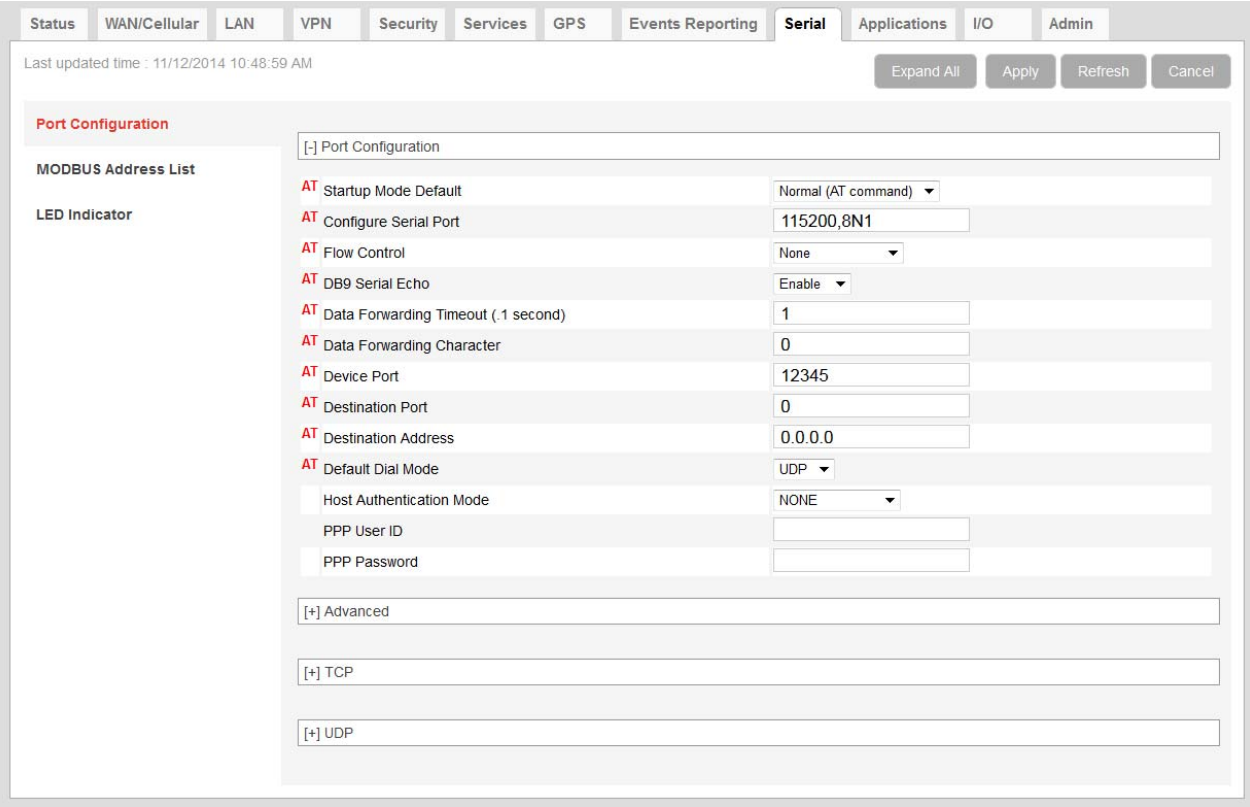


Figure 11-1: ACEmanager: Serial > Port Configuration > Port Configuration

Table 11-1: Serial Port Configuration > Port Configuration

Field	Description
Port Configuration	
Startup Mode Default	Default power-up mode for the serial port. When the AirLink device is power-cycled, the serial port enters the communication mode specified. *Note: It can take up to 5 minutes to establish a connection.* • Normal (AT command) default • PPP • UDP • TCP • Reverse Telnet/SSH—Allows you to telnet or SSH into a router or other device connected to the AirLink device via a serial port. For information on configuring reverse telnet, see Reverse Telnet/SSH on page 279. • Modbus ASCII • Modbus RTU (Binary) • BSAP—Bristol Standard Asynchronous Protocol • Variable Modbus • UDP Multiple Unicast—Data from the serial port is packed into UDP packets and sent to multiple IP addresses (for example, multiple AirLink devices). For more information, see UDP Multiple Unicast on page 281. You can also use an AT command to configure this field. See MD on page 430.
Autologin Reverse Telnet	This field only appears when the Startup Mode Default field is set to Reverse Telnet/SSH. Determines the log in procedure when using reverse telnet. • Enable—Do not enter a user name and password when you telnet to a a router or other device that has a serial connection to your AirLink device. Login is automatic. (default) • Disable—Enter a user name and password when you telnet to a a router or other device that has a serial connection to your AirLink device. For more information about reverse telnet, see Reverse Telnet/SSH on page 279.
Configure Serial Port	Format: [speed][data bits][parity][stop bits] Valid speeds are 300–115200, data bits: 7 or 8, parity: O,E,N,M, stop bits: 1,1.5. Default is 115200,8N1. You can also use an AT command to configure this field. See S23 on page 440.
Flow Control	Serial port flow control setting • None—No flow control is being used (default) • Hardware—RTS/CTS hardware flow control is being used • Transparent SW—Transparent software flow control. Uses escaped XON and XOFF for flow control. XON and XOFF characters in data stream are escaped with the @ character (0x40). @ in data is sent as @@. You can also use an AT command to configure this field. See \Q on page 439.

Table 11-1: Serial Port Configuration > Port Configuration

Field	Description
DB9 Serial Echo	AT command echo mode • Enable—Text is visible as you type (default) • Disable—Text you type is not visible You can also use an AT command to configure this field. See E on page 438.
Data Forwarding Timeout (.1 seconds)	The Data Forwarding Timeout feature causes ALEOS to wait until no data has been received on the serial port for the specified period of time beyond the built-in delay of 100 ms before sending a new PAD packet. Acceptable values are: 0–255. (Unit is 0.1 second; default is 1.) If the field is set to 0 or 1, the feature is disabled. ALEOS sends the new PAD packet after the built-in 100 ms delay. Data Forwarding Timeout is not applicable to AT and PPP modes.
Data Forwarding Character	PAD data forwarding character. ASCII code of character that causes data to be forwarded. Used in UDP or TCP PAD mode Default is 0 (No forwarding character). You can also use an AT command to configure this field. See S51 on page 433.
Device Port	The port on the AirLink device used for incoming TCP/UDP communication (Default is 12345) If either, or both, of the UDP Auto Answer or TCP Auto Answer parameters are enabled, when the AirLink device receives incoming TCP or UDP packets that are destined for this port, it strips off the IP header and send the packet payload out its serial port. You can also use an AT command to configure this field. See *DPORT on page 429.
Destination Port	The destination port that TCP/UDP communication is sent to You can also use an AT command to configure this field. See S53 on page 433.
Destination Address	IP address TCP/UDP communication is sent to You can also use an AT command to configure this field. See S53 on page 433.
Default Dial Mode	Protocol used to send messages Options are: • TCP • UDP (default) You can also use an AT command to configure this field. See S53 on page 433.
Host Authentication Mode	Sets the authentication method the host uses for PPP. Options are: • None (default) • CHAP—The stronger of the two protocols. Recommended, provided it is supported by all the client devices • PAP and CHAP—If CHAP is not supported by the client, the host reverts to PAP.
PPP User ID	Sets the User ID for authentication
PPP Password	Sets the User Password for authentication

For information on configuring an AirLink device to use SSH PAD mode, see SSH PAD Mode on page 23.

Reverse Telnet/SSH

The Reverse Telnet/SSH feature allows you to connect to and configure a router or other device that has a serial connection to your AirLink device.

You can have only one Reverse Telnet session open at a time. If a new Reverse Telnet session is started, any existing Reverse Telnet connection will be closed.

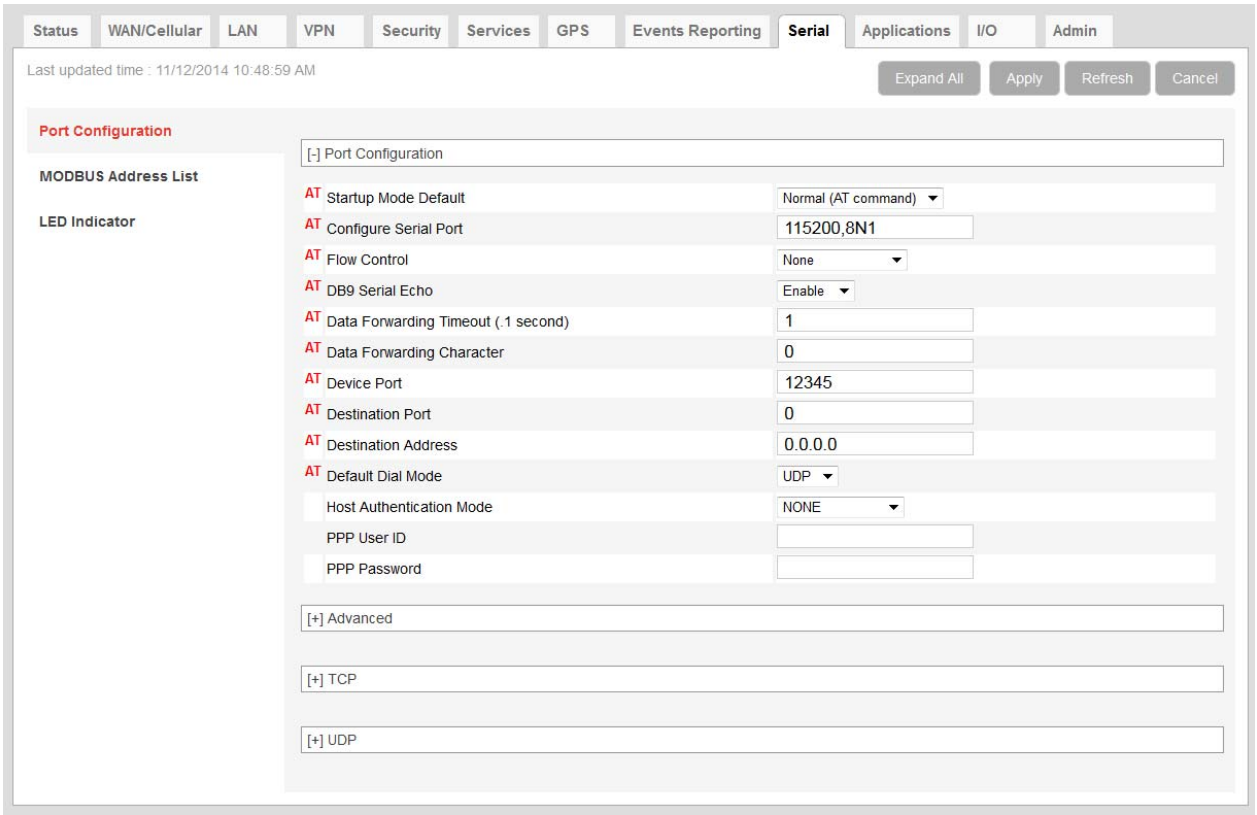
However, you can simultaneously have:

- One Telnet session for Reverse Telnet (using the port configured in the Device Port field on the Serial > Port Configuration page)
- One Telnet session for AT Commands (using the port configured in the Remote Login Server Telnet Port field on the Services > Telnet/SSH page)

Note: If you are using Reverse Telnet and you have VPNs, the more VPN tunnels in use, the greater the CPU load. This may result in lower throughput or greater delays.

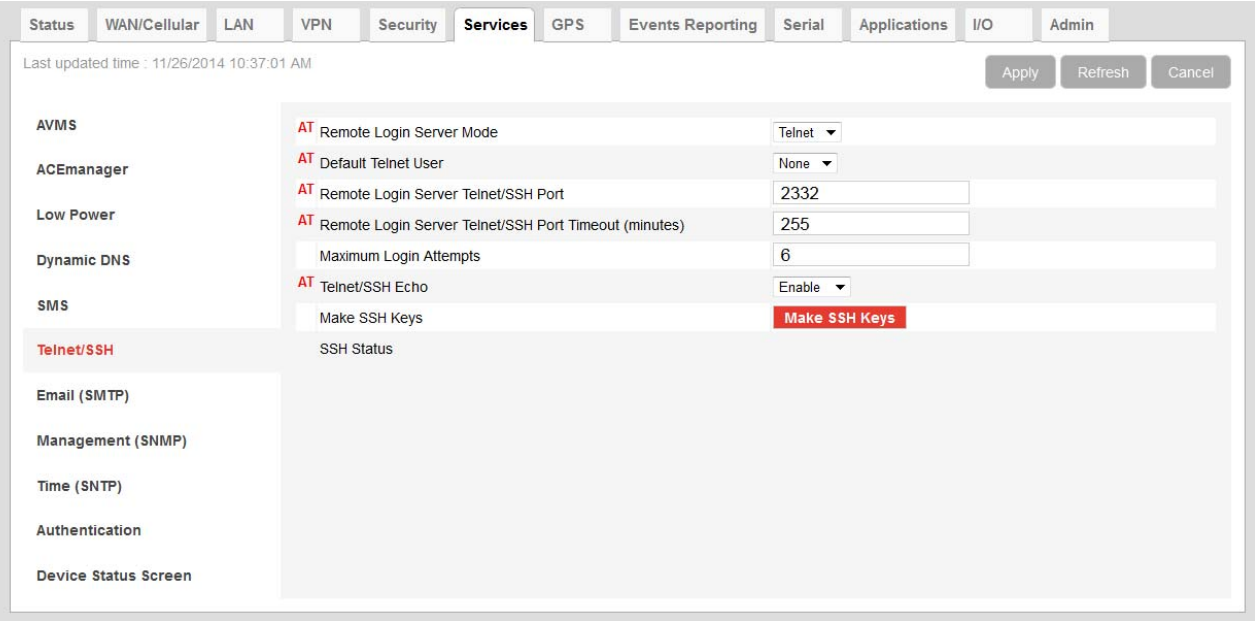
To configure Reverse Telnet/SSH:

1. Log into ACEmanager and go to Serial > Port Configuration.
2. In the Startup Mode Default field, select Reverse Telnet/SSH.
3. In the Configure Serial Port field, set the speed, data bits, parity, and stop bits. (The serial port configuration depends on the router you want to connect to. For example, to connect to a Cisco router that has a default baud rate of 9600, enter 9600,8N1 in the Configure Serial Port field.)

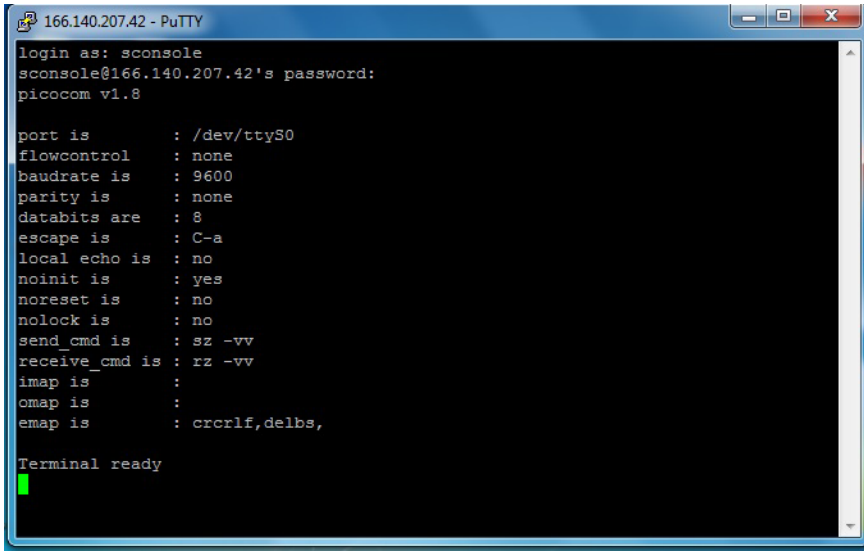


4. Optional—If you are planning to use telnet (rather than SSH), you can be automatically logged in when you telnet to the AirLink device without having to enter a user name and password. Autologin is not supported with SSH. To set up automatic login:
   a. In the Autologin Reverse Telnet field, select Enable.
   b. Click Apply.
5. Go to Services > Telnet/SSH.
6. In the Remote Login Server Mode field, select:
   - Telnet—if you want to Telnet into the connected device
   - SSH—if you want to SSH into the connected device

Note: If you enabled Autologin, select Telnet.



7. Click Apply.
8. Reboot the AirLink device.
9. Use a Telnet or SSH terminal client such as Putty or Teraterm to connect to the appropriate port:
   - If you are using Autologin, Telnet to the port specified in the Device Port field (default is 12345). SSH is not available with Autologin.
   - If you are not using Autologin, you can Telnet or SSH into the port specified in the Remote Login Server Telnet/SSH Port field (default is 2332).
10. If prompted, log in with the following credentials:
    - User name: sconsole
    - Password: 12345 (default)



For information on changing the default reverse telnet password, see Change Password on page 325.

ALEOS redirects you to the router or other device connected to the AirLink device serial port. You can use this connection to configure connected device.

Note: You may be required to enter a user name and password to access the router or other device.

UDP Multiple Unicast

With UDP Multiple Unicast, data from the serial port is packed into UDP packets and sent to multiple IP addresses. To configure UDP Multiple Unicast:

1. Log in to ACEmanager as “user” and go to Serial > Port Configuration > Port Configuration.
2. In the Startup Mode Default field, select UDP Multiple Unicast.
3. In the Destination Port field, enter the remote port to be used.
4. Click Apply.
5. Go to Serial > Modbus Address List and enter the index numbers and IP addresses of the devices you want the data sent to. (See Modbus Address List on page 289.)
6. Click Apply.
7. Reboot the device.

Note: To avoid flooding the network, there is a 20 millisecond pause between sending the UDP packet to each destination.

Advanced

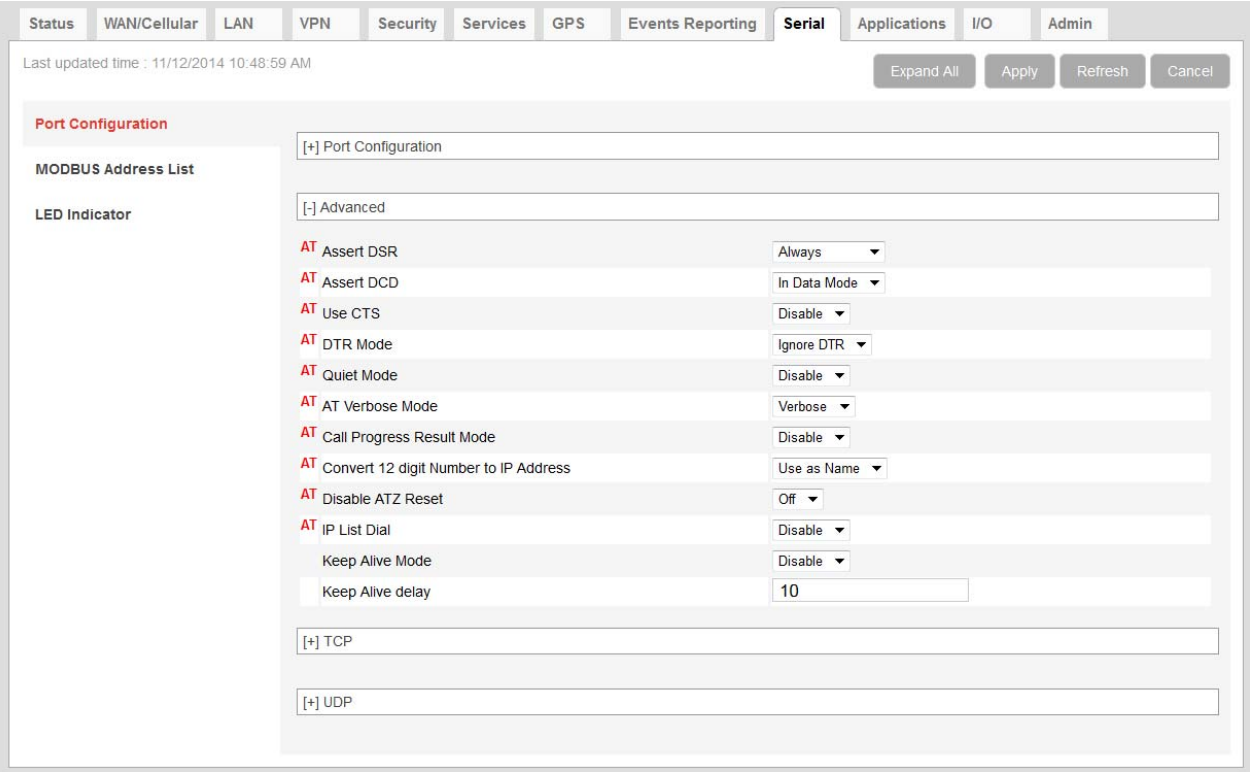


Figure 11-2: ACEmanager: Serial > Port Configuration > Advanced

Table 11-2: Serial Port Configuration > Advanced

Field	Description
Advanced	
Assert DSR	Assert DSR always when the device is in a data mode (UDP, TCP, etc.), or when the device is in network coverage. Options are: • Always (default) • In Data Mode • In Coverage You can also use an AT command to configure this field. See &S on page 439.
Assert DCD	Assert DCD always, or when the device is in a data mode (UDP, TCP, etc.) or when the device is in network coverage. Options are: • Always • In Data Mode (default) • In Coverage You can also use an AT command to configure this field. See &C on page 436.

Table 11-2: Serial Port Configuration > Advanced

Field	Description
Use CTS	Assert CTS when there is network coverage. Options are: • Disable (default) • Enable You can also use an AT command to configure this field. See *CTSE on page 429.
DTR Mode	Use DTR from the serial device, or ignore DTR (same as S211 on page 441). Options are: • Use DTR • Ignore DTR (default)
Quiet Mode	Disable or enable display of device responses. Options are: • Disable (default) • Enable You can also use an AT command to configure this field. See Q on page 438.
AT Verbose Mode	Sets the level of information returned for AT commands Options are: • Verbose (default) • Numeric You can also use an AT command to configure this field. See V on page 441.
Call Progress Result Mode	When enabled adds 19200 to CONNECT messages Options are: • Disable (default) • Enable You can also use an AT command to configure this field. See X on page 441.
Convert 12 digit Number to IP Address	Choose whether a 12-digit number is converted to an IP address (eg. 111222333444 to 111.222.333.444). Options are: • Use as Name (default) • Use as IP You can also use an AT command to configure this field. See *NUMTOIP on page 433
Disable ATZ Reset	The value set in this field determines whether or not issuing an ATZ Command resets the AirLink device. Options are: • On — Block is enabled—ATZ does not reset the device. • Off —Block is disabled—ATZ resets the device. (default) You can also use an AT command to configure this field. See *DATZ on page 438.
IP List Dial	This allows access to the Modbus IP Address using the first two digits of the dial string. For example, ATDT1234567 would imply ID index 12 on the Modbus Address list and use the associated IP Address as the destination. Options are: • Disable (default) • Enable You can also use an AT command to configure this field. See IPL on page 432.

Table 11-2: Serial Port Configuration > Advanced

Field	Description
Keep Alive Mode	When this feature is enabled, the AirLink device reboots if there is no traffic for longer than the period configured in the Keep Alive Delay field. Options are” • Disable (default) • Enable
Keep Alive delay	When Keep Alive Mode is enabled, use this field to set the delay (in minutes) before the AirLink device reboots if there is no traffic on the serial port. Accepted values: • 10–65535 (Default is 10.)

TCP

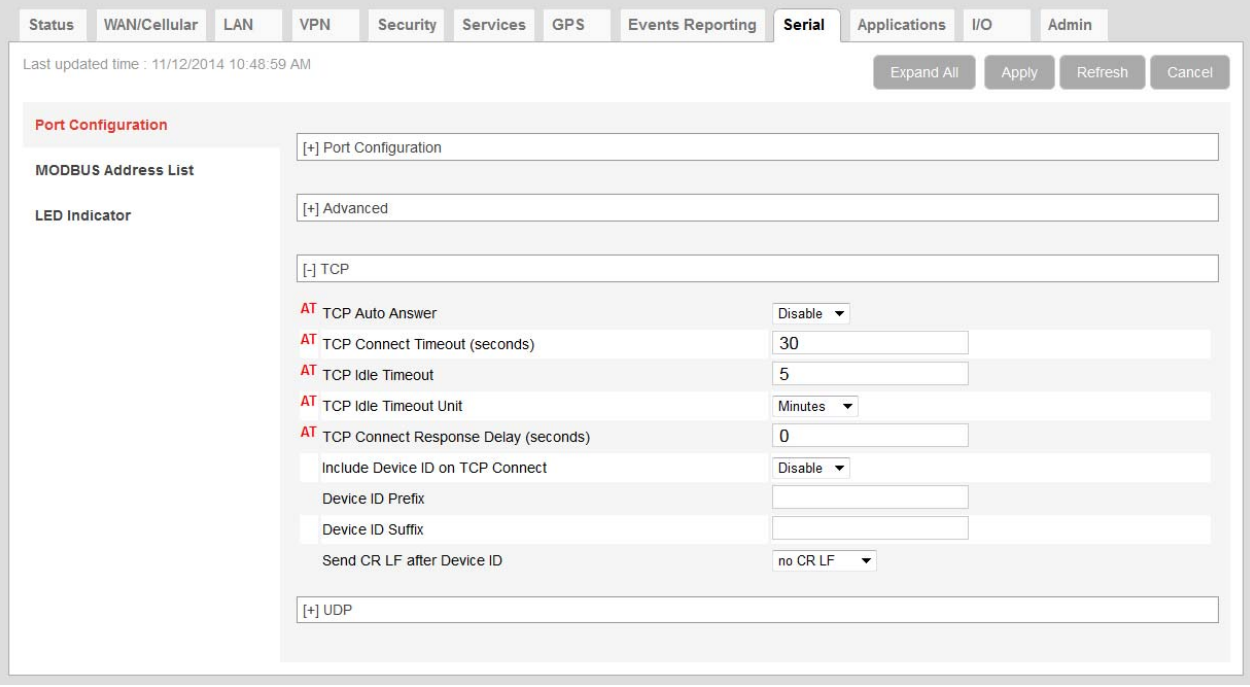


Figure 11-3: ACEmanager: Serial > Port Configuration > TCP

Table 11-3: Serial Port Configuration > TCP

Field	Description
TCP	
TCP Auto Answer	This determines how the AirLink device responds to an incoming TCP connection request. The AirLink device remains in AT Command mode until a connection request is received. The AirLink device sends a “RING” string to the host. A “CONNECT” sent to the host indicates acknowledgment of the connection request and the TCP session is established. • Disable (default) • Enable You can also use an AT command to configure this field. See S0 on page 439.

Table 11-3: Serial Port Configuration > TCP

Field	Description
TCP Connect Timeout (seconds)	Specifies the number of seconds to wait for a TCP connection to be established when dialing out (Default is 30.) You can also use an AT command to configure this field.
TCP Idle Timeout	TCP idle time-out in the configured units (See TCP Idle Timeout Unit on page 285.) Specifies a time interval upon which if there is no in or outbound traffic through a TCP connection, the connection is terminated. Default is 5. You can also use an AT command to configure this field. See TCPT on page 434.
TCP Idle Timeout Unit	Units used for the TCP Idle Timeout Interval. Options are: • Minutes (default) • Seconds You can also use an AT command to configure this field. See TCPS on page 434.
TCP Connect Response Delay (seconds)	The number of seconds to delay the “CONNECT' response upon establishing a TCP connection, or the number of tenths of seconds to delay before outputting ENQ on the serial port after the CONNECT when the ENQ feature is enabled. • 0–255 (Default is 0.) You can also use an AT command to configure this field. See S221 on page 441.
Include Device ID on TCP Connect	If this option is enabled, after a TCP connection is established, ALEOS sends a packet that contains the device ID (and optionally a prefix, suffix, and CRLF). Options are: • Disable (default) • Enable *Note: To use this feature, ensure that the Device ID is configured in the Use Device ID in Location Reports field on the GPS screen (GPS > Global Settings > General). See Global Settings on page 253.*
Device ID Prefix	Sets the Prefix DID in the device identification packet upon TCP connection. Maximum length of the prefix is 80 characters.
Device ID Suffix	Sets the Suffix DID in the device identification packet upon TCP connection. Maximum length of the suffix is 80 characters.
Send CR LF after Device ID	Enables a carriage return to be inserted in the device identification packet after the Suffix DID. Options are: • no CR LF • send CR • send CR LF (carriage return, line feed) Default

UDP

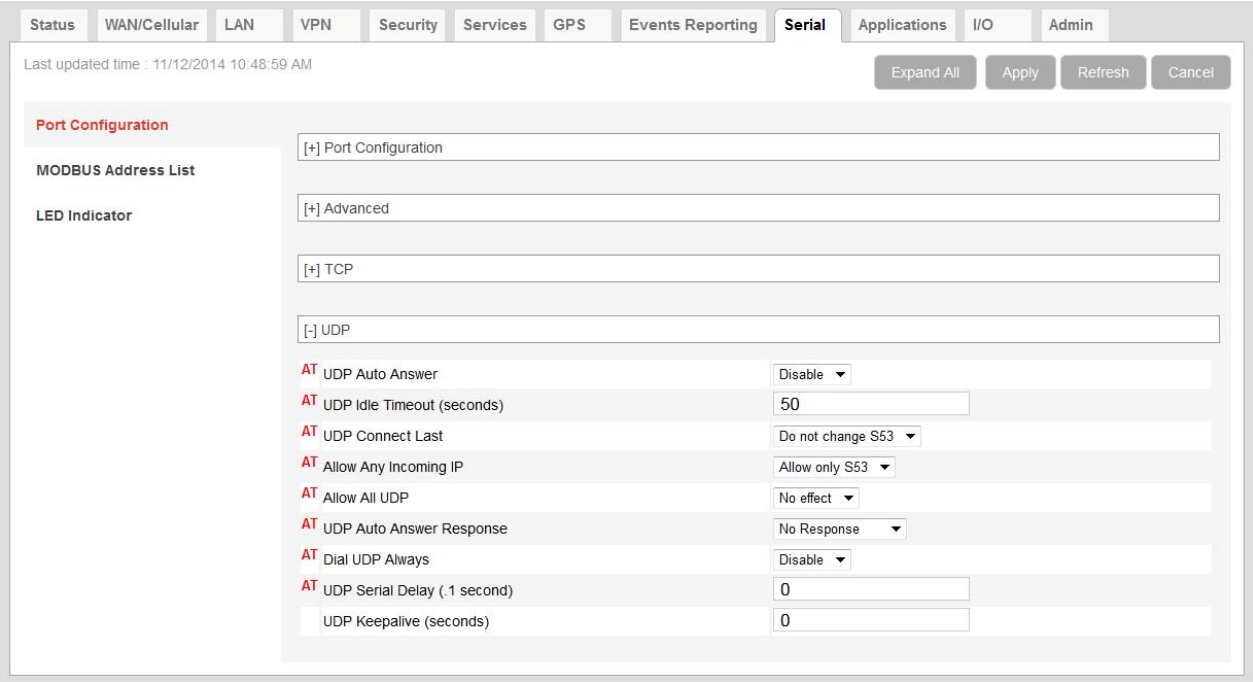


Figure 11-4: ACEmanager: Serial > Port Configuration > UDP

Table 11-4: Serial Port Configuration > UDP

Field	Description
UDP	
UDP Auto Answer	Whether the AirLink device auto answers and incoming UDP connection request Options are: • Disable (default) • Enable You can also use an AT command to configure this field. See S82 on page 434.
UDP Idle Timeout (seconds)	UDP Idle Time-out in seconds Specifies a time interval upon which if there is no in or outbound traffic through a UDP connection, the connection is terminated. • 0— No idle time-out • 1–255 Time-out in seconds (Default is 50.) You can also use an AT command to configure this field. See S83 on page 434.

Table 11-4: Serial Port Configuration > UDP

Field	Description
UDP Connect Last	Allows you to choose to use the last accepted IP address and port number as the default settings, instead of using S53 (destination address) Options are: • Do not change S53 (default) • Set S53 last IP *Note: Resetting the device restores the configured S53 (destination address).* You can also use an AT command to configure this field. See *UDPLAST on page 435.
Allow Any Incoming IP	When UDP auto answer is enabled, use this field to select whether to allow any incoming IP address to connect or to only allow the configured destination IP address to connect. Options are: • Allow only S53 (default) • Allow any IP address If you select Allow only S53, the Destination Port and Destination Address fields under Serial > Port Configuration must be configured. (See Table 11-1 on page 277.) You can also use an AT command to configure this field. See AIP on page 429.
Allow All UDP	Accepts UDP packets from all IP addresses when a UDP session is active. If there is no UDP session active, an incoming UDP packet is treated according to the UDP auto answer and AIP settings. Options are: • No effect (default) • Allow all—The AirLink device accepts all UDP traffic from any IP address during a UDP session. You can also use an AT command to configure this field. See *UALL on page 434.
UDP Auto Answer Response	Half-Open Response—In UDP auto answer (half-open) mode. Options are: • No Response—No Response codes when UDP session is initiated (default) • RING CONNECT—RING CONNECT response codes sent out serial link before the data from the first UDP packet *Note: Quiet Mode must be Off.* You can also use an AT command to configure this field. See HOR on page 438.
Dial UDP Always	The dial command always uses UDP, even when using ATDT. Options are: • Disable—Dial using the means specified (default) • Enable—Dial UDP always, even when using ATDT *Note: When this parameter is set you cannot establish a TCP PAD connection.* You can also use an AT command to configure this field. See *DU on page 429.

Table 11-4: Serial Port Configuration > UDP

Field	Description
UDP Serial Delay (.1 second)	Waits the specified delay before sending the first received UDP packet and the subsequent UDP packets out to the port Ethernet (in 100 ms units). • No UDP packet delay (default) • 1–255— Delay in 100ms units, from 100 ms to 25.5 sec. You can also use an AT command to configure this field. See *USD on page 435.
UDP Keepalive (seconds)	Use this field to configure the time interval (in seconds) for sending UDP keepalive packets. Options are: • 1–65535—ALEOS sends a UDP packet, containing the AirLink device's IMEI (in little endian) to the configured Destination IP Address:Destination Port when the UDP connection is first established and then at the configured interval. If the AirLink devices WAN IP address changes, a UDP packet is sent and the timer is reset. • 0—UDP Keepalive is disabled. (default)

PPP

Use Point-to-Point Protocol (PPP) to establish a connection between a host PC serial port and the AirLink device, as shown in Figure 11-5.

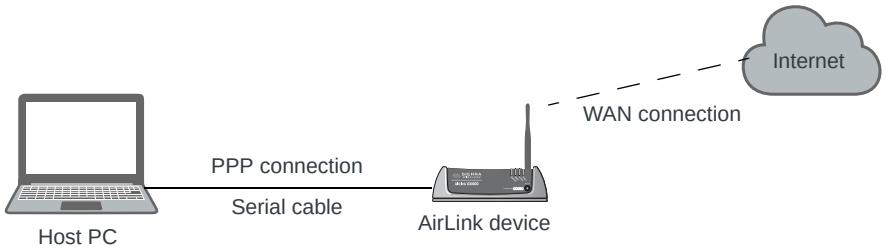


Figure 11-5: PPP connection

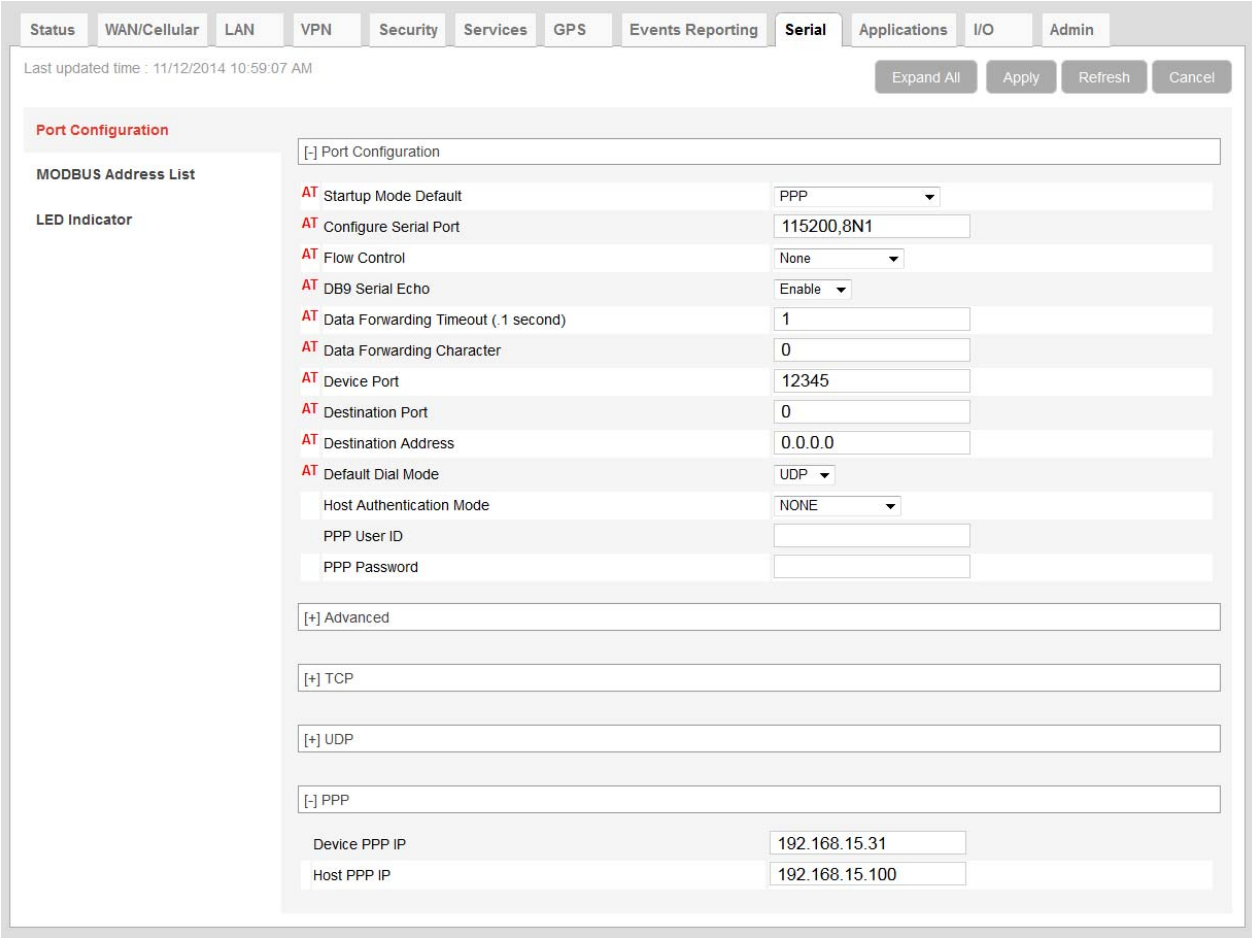


Figure 11-6: ACEmanager: Serial > Port Configuration > PPP

Table 11-5: Serial Port Configuration > PPP

Field	Description
PPP[a]	
Device PPP IP	Sets the device IP address (in private mode)
Host PPP IP	Sets the host IP address (in private mode)

a. Note: This section is only visible when PPP is selected in the Startup Mode Default field.

Modbus Address List

To add a Modbus Address:

1. Log in to ACEmanager as “user” and go to Serial > MODBUS Address List.
2. Click Add More.
3. Enter the Index number, an equal sign, and the IP address. For example: 10=123.123.123.123 (decimal)

0xA=123.123.123.123 (hex) Prefix 0x to hex numbers.

Including the port number after the IP address is optional. If you include the port number, separate the port number and IP address by a colon.
For example:

10=123.123.123.123:11223

0xA=123.123.123.123:11223

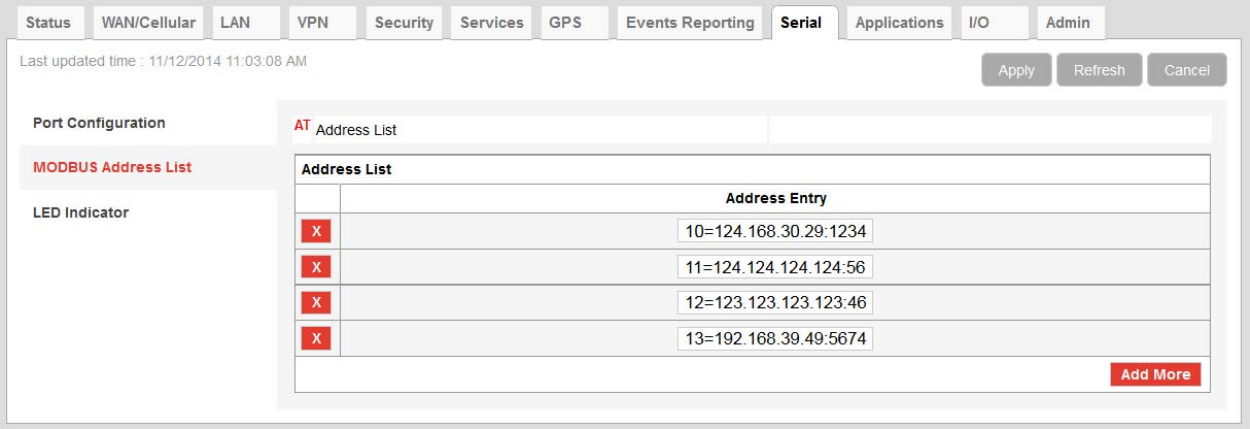


Figure 11-7: Serial > MODBUS Address List

4. Click Apply.
5. Reboot.

To delete an address from the list, click the X beside it.

Note: You can also use the AT Commands MLIST and MLISTX to add address entries and MLIST? or MLISTX? to query the entries on the list. See MLIST on page 431, and MLISTX on page 431.

I/O X-Card Serial Port Configuration

This section applies only to the AirLink GX Series device with an I/O X-Card installed. The serial port on the I/O X-Card is a 5-pin RS232 port supporting the following signals: TX, RTS, CTS, and GND. The following signals are not supported: RI, DCD, DTR, and DSR.For more information on the I/O X-Card, refer to the AirLink GX Series User Guide.

The I/O X-Card supports AT Command mode, TCP and UDP connections. The following ALEOS features are not supported on the I/O X-Card serial port:

- PPP
- Reverse Telnet/SSH
- Modbus
- BSAP
- UDP Multiple Unicast
- Keep alive mode
- Device ID included in TCP packets

To configure the serial port for the installed I/O X-Card:

1. In ACEmanager, go to Serial > I/O X-Card Serial Port.

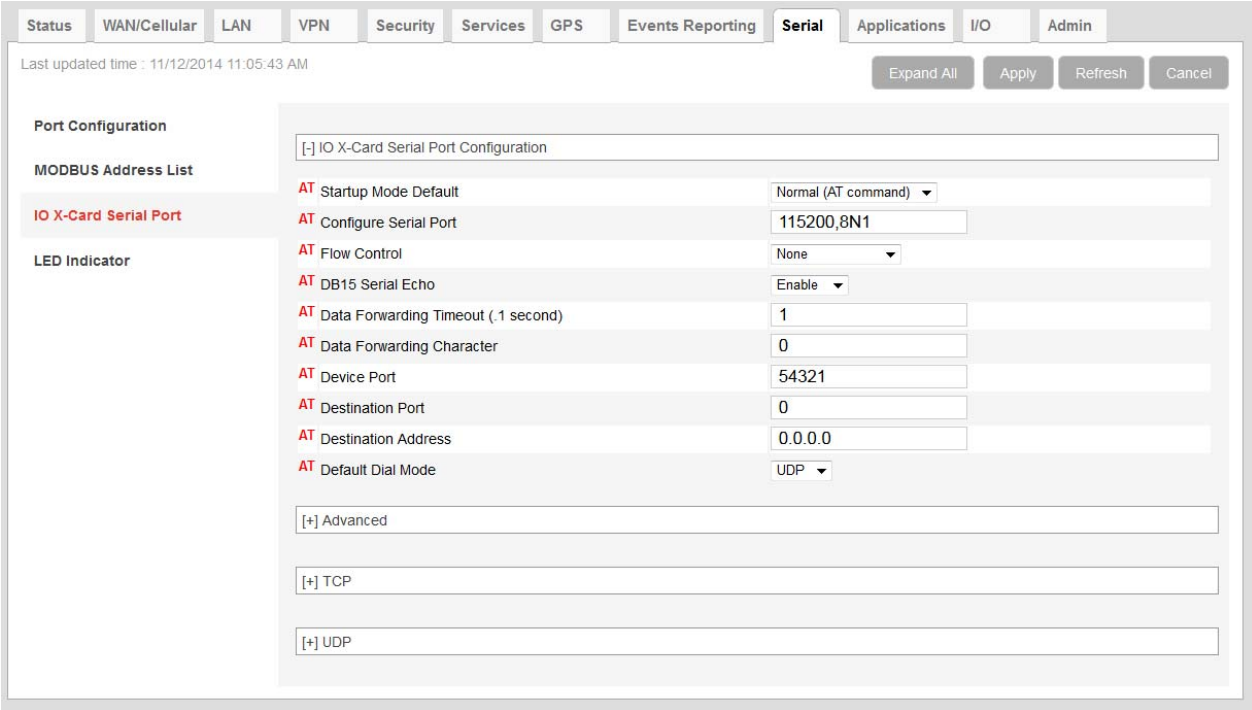


Figure 11-8: ACEmanager: Serial > IO X-Card Serial Port > IO X-Card Serial Configuration

Table 11-6: Serial > IO X-Card Serial Port > IO X-Card Serial Configuration

Field	Description
Startup Mode Default	The default startup mode for the serial port Options are: • Normal (AT command) default • UDP • TCP You can also use an AT command to configure this field. See MD on page 430.
Configure Serial Port	Format: [speed],[data bits][parity][stop bits] Valid speeds are 300–115200, data bits: 7 or 8, parity: O,E,N,M, stop bits: 1,1.5,2 • 115200, 8N1 (default) You can also use an AT command to configure this field. See S23 on page 440.
Flow Control	Serial port data flow control setting • None—No flow control is being used (default) • Hardware—RTS/CTS hardware flow control is being used • Transparent SW—Transparent software flow control. Uses escaped XON and XOFF for flow control. XON and XOFF characters in data stream are escaped with the @ character (0x40). @ in data is sent as @@. You can also use an AT command to configure this field. See \Q on page 439.

Table 11-6: Serial > IO X-Card Serial Port > IO X-Card Serial Configuration

Field	Description
DB15 Serial Echo	AT command echo mode Options are: • Enable—Text is visible as you type. (default) • Disable—Text you type is not visible. You can also use an AT command to configure this field. See E on page 438.
Data Forwarding Timeout (.1 second)	Data forwarding time-out. (How long the application waits before bundling characters to send) If set to 0, a forwarding time-out of 10ms is used. Used in UDP or TCP PAD mode. Increments in tenths of a second. Default is 1 (The forwarding time-out is 100 ms.) You can also use an AT command to configure this field. See S50 on page 433.
Data Forwarding Character	PAD data forwarding character. ASCII code of character that causes data to be forwarded. Used in UDP or TCP PAD mode Default is No forwarding character You can also use an AT command to configure this field. See S51 on page 433.
Device Port	The port on the AirLink device used for incoming TCP/UDP communication (Default is 54321) If either, or both, of the UDP Auto Answer or TCP Auto Answer parameters are enabled, when the AirLink device receives incoming TCP or UDP packets that are destined for this port, it strips off the IP header and send the packet payload out the serial port on the I/O X-Card. You can also use an AT command to configure this field. See *DPORT on page 429.
Destination Port	The destination port that TCP/UDP communication is sent to You can also use an AT command to configure this field. See S53 on page 433.
Destination Address	The IP address TCP/UDP communication is sent to You can also use an AT command to configure this field. See S53 on page 433.
Default Dial Mode	Protocol used to send messages Options are: • TCP • UDP (default) You can also use an AT command to configure this field. See S53 on page 433.

Advanced Settings

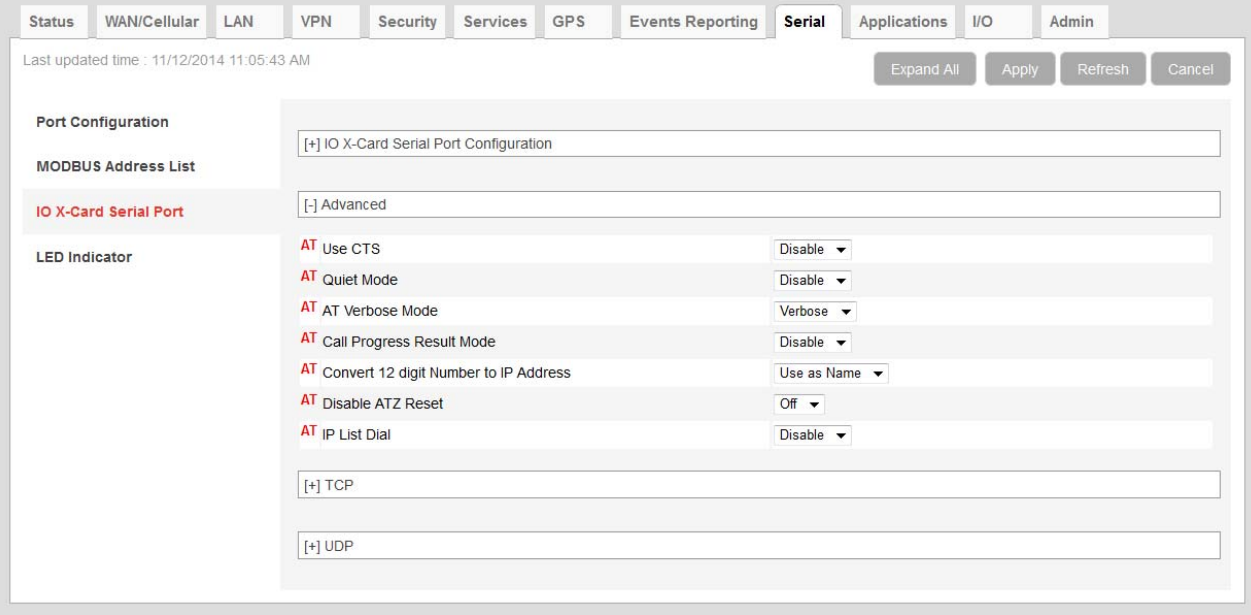


Figure 11-9: ACEmanager: Serial > IO X-Card Serial Port > Advanced

Table 11-7: Serial > X-Serial Port Configuration >Advanced and TCP Configuration

Field	Description
Use CTS	Assert CTS when there is network coverage. Options are: • Disable (default) • Enable You can also use an AT command to configure this field. See *CTSE on page 429.
Quiet Mode	Disable or enable display of device responses. Options are: • Enable • Disable (default) You can also use an AT command to configure this field. See Q on page 438.
AT Verbose Mode	Sets the level of information returned for AT commands Options are: • Verbose (default) • Numeric You can also use an AT command to configure this field. See V on page 441.
Call Progress Result Mode	When enabled adds 19200 to CONNECT messages. Options are: • Enable • Disable (default) You can also use an AT command to configure this field. See X on page 441.

Table 11-7: Serial > X-Serial Port Configuration >Advanced and TCP Configuration

Field	Description
Convert 12 digit Number to IP Address	Choose whether or not a 12-digit number is converted to an IP address For example, converts 111222333444 to 111.222.333.444 Options are: • Use as Name (default) • Use as IP You can also use an AT command to configure this field. See *NUMTOIP on page 433.
Disable ATZ Reset	The value set in this field determines whether or not issuing an ATZ Command resets the AirLink device. Options are: • On (default) — ATZ does not reset the AirLink device • Off —ATZ resets the AirLink device. You can also use an AT command to configure this field. See *DATZ on page 438.
IP List Dial	This allows access to the Modbus IP Address using the first two digits of the dial string. For example, ATDT1234567 would imply ID index 12 on the Modbus Address list and use the associated IP Address as the destination. Options are: • Enable • Disable (default) You can also use an AT command to configure this field. See IPL on page 432.

TCP Settings

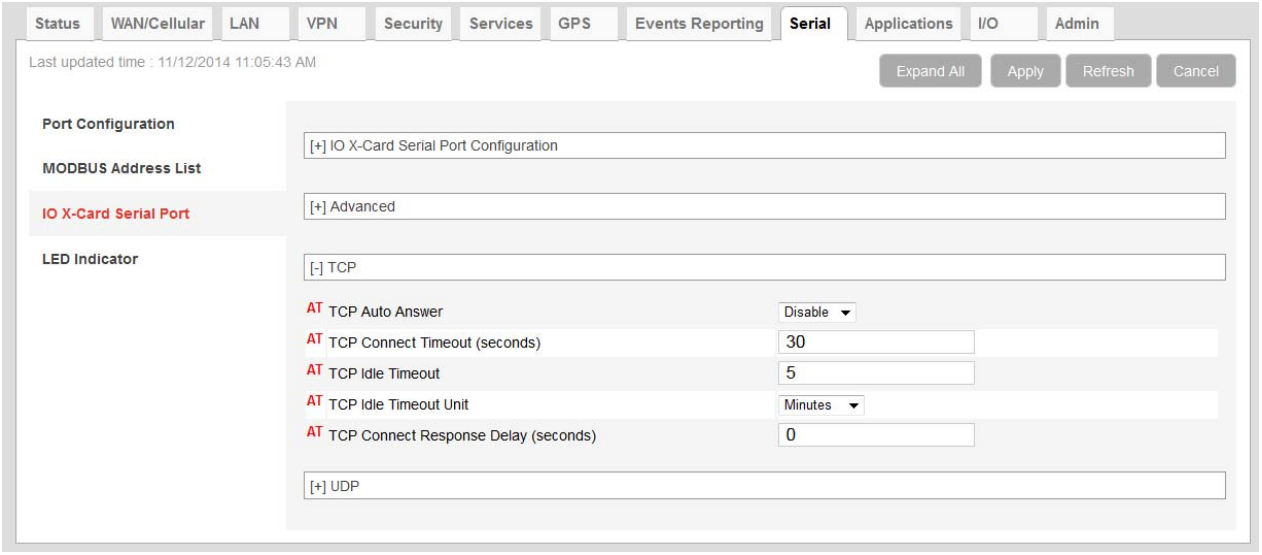


Figure 11-10: ACEmanager: Serial > IO X-Card Serial Port > TCP

Table 11-8: Serial > X-Serial Port Configuration > Advanced and TCP Configuration

Field	Description
TCP Auto Answer	This determines how the AirLink device responds to an incoming TCP connection request. The AirLink device remains in AT Command mode until a connection request is received. The AirLink device sends a “RING” string to the host. A “CONNECT” sent to the host indicates acknowledgment of the connection request and the TCP session is established. Options are: • Enable • Disable (default) You can also use an AT command to configure this field. See S0 on page 439.
TCP Connect Timeout (seconds)	Specifies the number of seconds to wait for a TCP connection to be established when dialing out You can also use an AT command to configure this field.
TCP Idle Timeout	TCP idle time-out in the configured units (See TCP Idle Timeout Unit on page 285.) Specifies a time interval upon which if there is no in or outbound traffic through a TCP connection, the connection is terminated. Default is 5. You can also use an AT command to configure this field. See TCPT on page 434.
TCP Idle Timeout Unit	Units used for the TCP Idle Timeout interval Options are: • Minutes (default) • Seconds You can also use an AT command to configure this field. See TCPS on page 434.
TCP Connect Response Delay (seconds)	The number of seconds to delay the “CONNECT' response upon establishing a TCP connection, or the number of tenths of seconds to delay before outputting ENQ on the serial port after the CONNECT when the ENQ feature is enabled. • n=0–255 You can also use an AT command to configure this field. See S221 on page 441.

UDP Settings

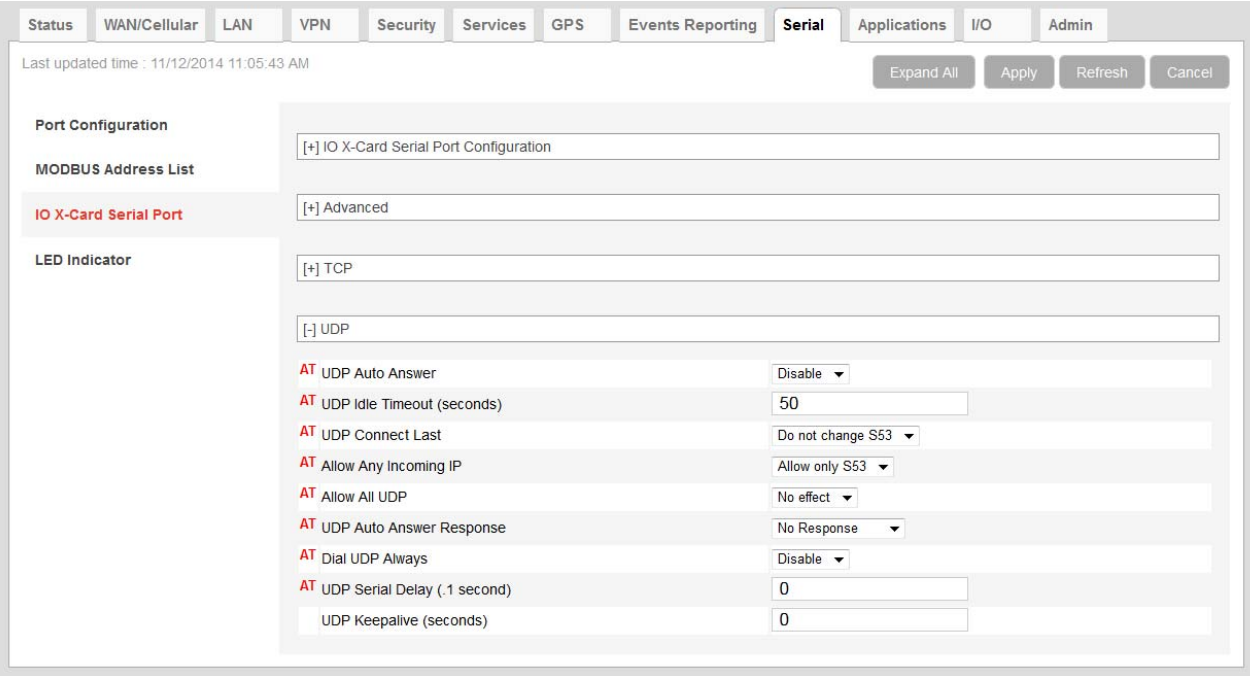


Figure 11-11: ACEmanager: Serial > IO X-Card Serial Port > UDP

Table 11-9: Serial > IO X-Card Serial Port > UDP

Field	Description
UDP Auto Answer	Whether the AirLink device auto answers an incoming UDP connection request Options are: • Enable • Disable (default) You can also use an AT command to configure this field. See S82 on page 434.
UDP Idle Timeout (seconds)	UDP idle time-out in seconds Specifies a time interval upon which if there is no in or outbound traffic through a UDP connection, the connection is terminated. Default is 50. You can also use an AT command to configure this field. See S83 on page 434.
UDP Connect Last	Allows you to choose to use the last accepted IP address and port number as the default settings, instead of using S53 (destination address) Options are: • Do not change S53 — Does not change the destination IP address (default) • Set S53 as last —Uses the last accepted IP address *Note: Resetting the device restores the configured S53 (destination address).* You can also use an AT command to configure this field. See *UDPLAST on page 435.

Table 11-9: Serial > IO X-Card Serial Port > UDP

Field	Description
Allow Any Incoming IP	When UDP auto answer is enabled, use this field to select whether to allow any incoming IP address to connect or to only allow the configured destination IP address to connect. Options are: • Allow only S53 —Allows only the configured destination IP address (default) • Allow any IP If you select Allow only S53, the Destination Port and Destination Address fields under Serial > X-Serial Port Configuration must be configured (See Table 11-6 on page 291.) You can also use an AT command to configure this field. See AIP on page 429.
Allow All UDP	Accepts UDP packets from all IP addresses when a UDP session is active. If there is no UDP session active, an incoming UDP packet is treated according to the UDP auto answer and AIP settings. Options are: • No effect (default) • Allow all—The AirLink device accepts all UDP traffic from any IP address during a UDP session You can also use an AT command to configure this field. See *UALL on page 434.
UDP Auto Answer Response	Half-Open Response—In UDP auto answer (half-open) mode. Options are: • No Response—No Response codes when UDP session is initiated (default) • RING CONNECT—RING CONNECT response codes sent out over the serial link before the data from the first UDP packet *Note: Quiet Mode must be Off.* You can also use an AT command to configure this field. See HOR on page 438.
Dial UDP Always	The dial command always uses UDP, even when using ATDT. Options are: • Disable—Dial using the method specified (default) • Enable—Dial UDP always, even when using ATDT *Note: When this parameter is set you cannot establish a TCP PAD connection.* You can also use an AT command to configure this field. See *DU on page 429.

Table 11-9: Serial > IO X-Card Serial Port > UDP

Field	Description
UDP Serial Delay (.1 seconds)	Waits the specified delay before sending the first received UDP packet and the subsequent UDP packets out to the Ethernet port (in 100 ms units). • No UDP packet delay (default) • 1–255 — Delay in 100 ms units, from 100 ms to 25.5 sec. You can also use an AT command to configure this field. See *USD on page 435.
UDP Keepalive (seconds)	Use this field to configure the time interval (in seconds) for sending UDP keepalive packets. Options are: • 1–65535—ALEOS sends a UDP packet, containing the AirLink device's IMEI (in little endian) to the Destination IP Address:Destination Port configured on the I/O X-Card when the UDP connection is first established and then at the configured interval. If the AirLink devices WAN IP address changes, a UDP packet is sent and the timer is reset. • 0—UDP Keepalive is disabled.

Configuring IP to Serial with Auto Answer and Serial to IP

You can configure the AirLink device to:

- Auto Answer incoming TCP/IP or UDP/IP connections and send the packet payload out the AirLink device's serial port to a connected device
- Create and send TCP/IP or UDP/IP packets containing payload data that the AirLink device receives over its serial port from a connected device
- Both receive and send TCP/IP or UDP/IP packets (that is, both of the above functionalities)

If you have a GX Series device with an I/O X-Card installed, you can also configure this feature on the I/O X-Card serial port.

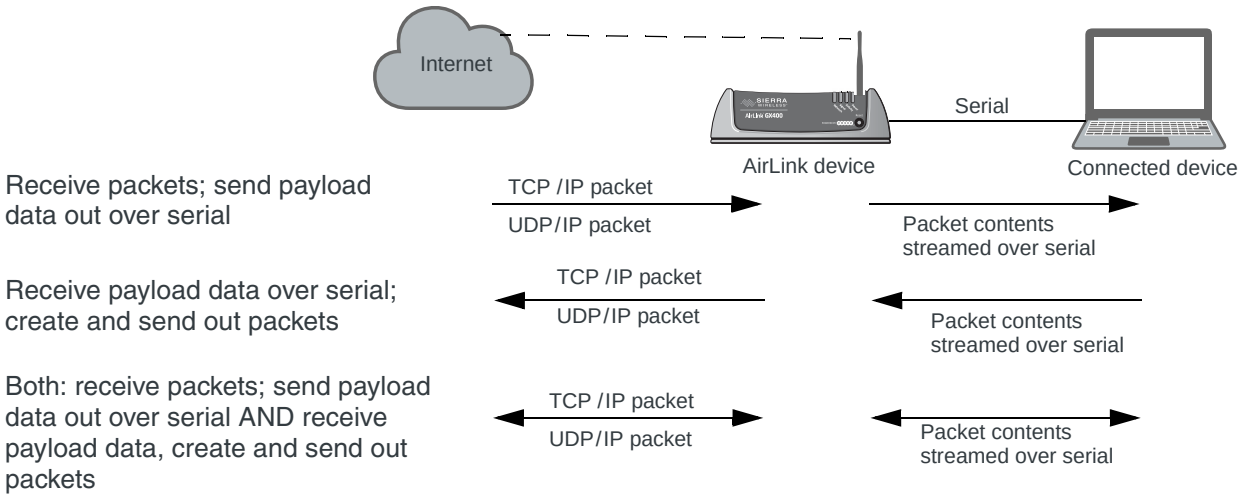
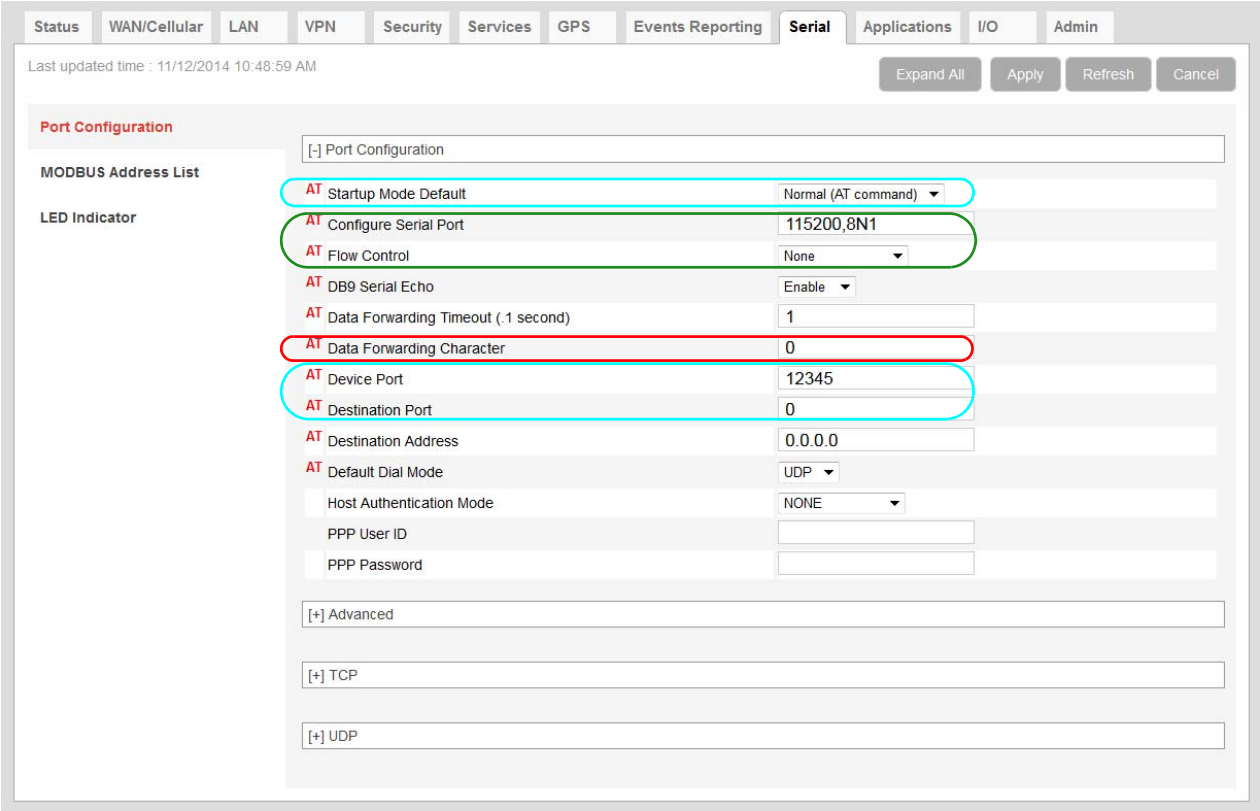

Internet
Serial
AirLink device
Connected device
Receive packets; send payload data out over serial
TCP /IP packet
UDP/IP packet
Packet contents streamed over serial
Receive payload data over serial; create and send out packets
TCP /IP packet
UDP/IP packet
Packet contents streamed over serial
Both: receive packets; send payload data out over serial AND receive payload data, create and send out packets
TCP /IP packet
UDP/IP packet
Packet contents streamed over serial

Figure 11-12: TCP and UDP Auto Answer

To configure the AirLink device for TCP/UDP auto answer, sending IP packets or both:

1. In ACEmanager, go to Serial > Port Configuration. If you are configuring an I/O X-Card, go to Serial > I/O X-Card Serial Port.



Required fields for receiving data payloads over serial, creating IP packets to send

Required fields for receiving IP packets and sending out data payloads over serial

Required fields both receiving data payloads over serial, creating IP packets to send and receiving data payloads over serial, creating IP packets to send

Figure 11-13: ACEmanager: Serial > Port Configuration

2. Use Table 11-10 and the instructions following the table to configure the desired options for this feature.

Table 11-10: Quick Guide to Configuring IP to Serial with Auto Answer and Serial to IP

Field	To receive packets and send data payload out over serial	To receive data payloads over serial and send out packets	Both (to receive packets - send out data payload AND receive data payload and send out packets)
Startup Mode Default See step Step 3.	N/A	UDP or TCP	UDP or TCP
Configure Serial Port See Step 4.	115200,8N1	115200,8N1	115200,8N1

Table 11-10: Quick Guide to Configuring IP to Serial with Auto Answer and Serial to IP

Field	To receive packets and send data payload out over serial	To receive data payloads over serial and send out packets	Both (to receive packets - send out data payload AND receive data payload and send out packets)
Flow Control See Step 5.	None	None	None
Device Port See Step 6.	12345 54321 for I/O X-Card	N/A	12345 54321 for I/O X-Card
Destination Port See Step 7.	N/A	Required	Required
Destination Address See Step 8.	N/A	Required	Required

3. Startup Default Mode—When the Startup Mode is set to UDP or TCP, the AirLink device takes any data sent to its serial port by a connected device and encapsulates it into a TCP/IP or UDP/IP packet.
4. Configure Serial Port—Set the baud rate of the serial port on the AirLink device so that it matches the baud rate of the serial port on the connected device. (The default baud rate is 115200 bps.) You can also use this field to set the framing characteristics for the serial port communication on those rare occasions when the default value of 8N1 does not apply.
5. Flow Control—This field can usually be left at the default value (None) as most serial devices use only a 3-wire connection (Tx, RX, and Gnd). However, if the serial device uses the RTS and CTS pins on the serial connection to control data flow between the two devices, set this field to Hardware.
6. Device Port—Data received on a TCP/IP or UDP/IP connection to the configured Device Port is sent out the serial port. The default value for the port:
   - On the AirLink device is 12345
   - On the I/O X-Card is 54321
7. Destination Port—The AirLink device uses the port value specified in this field to determine which port it sends the IP packet containing the data payload to. The AirLink device enters the value in the Destination Port field in the header of the IP packet it creates.
8. Destination Address—The AirLink device uses the IP address specified in this field to determine the IP address to send the packet it creates to. The AirLink device enters this IP address in the header of the IP packet it creates.
9. If you are configuring the AirLink device to:
   - Create and send packets only, go to step Step 10.
   - Receive TCP/UDP packets, complete the following instructions.

For Receiving TCP/IP Packets:

a. Expand the +TCP section of the screen.

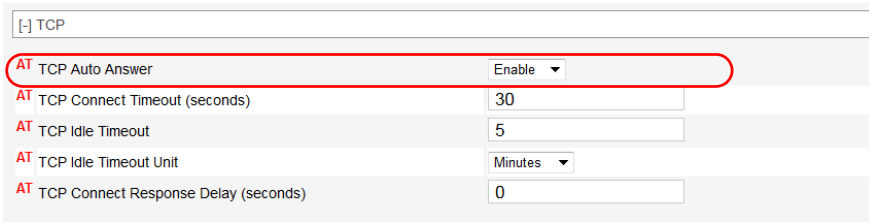


Figure 11-14: ACEmanager: Serial > Port Configuration > TCP

b. Set the TCP Auto Answer field to Enable.

For Receiving UDP/IP Packets:

a. Expand the +UDP section of the screen.

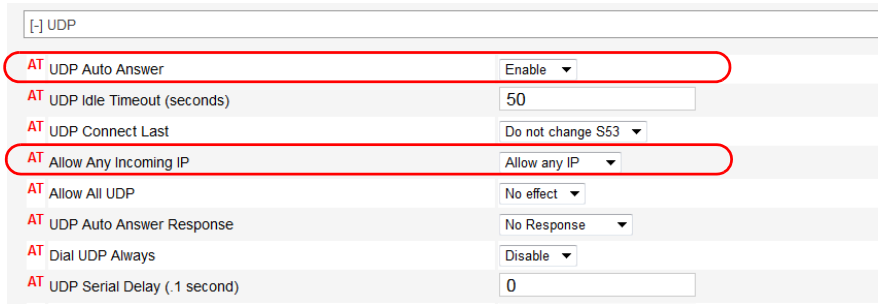


Figure 11-15: ACEmanager: Serial > Port Configuration > UDP

b. Set the UDP Auto Answer field to Enable.

c. Set the Allow Any Incoming IP field to Allow Any IP. (If this field is left at the default value, the AirLink device only accepts incoming UDP/IP packets from the IP address specified in the Destination Address field in the Port Configuration section of the screen.

10. For information on the other parameters, see Port Configuration on page 275.

11. Click Apply.

12. Click Reboot (in the upper right of the screen).

13. Once the reboot is complete, this feature is enabled.

If the packet contents are not being sent to the connected device, see the troubleshooting information in TCP/IP and UDP/IP Auto Answer on page 467.

LED Indicator

You can configure the Activity LED on the AirLink device to flash red when traffic is being transmitter or received over the serial port.

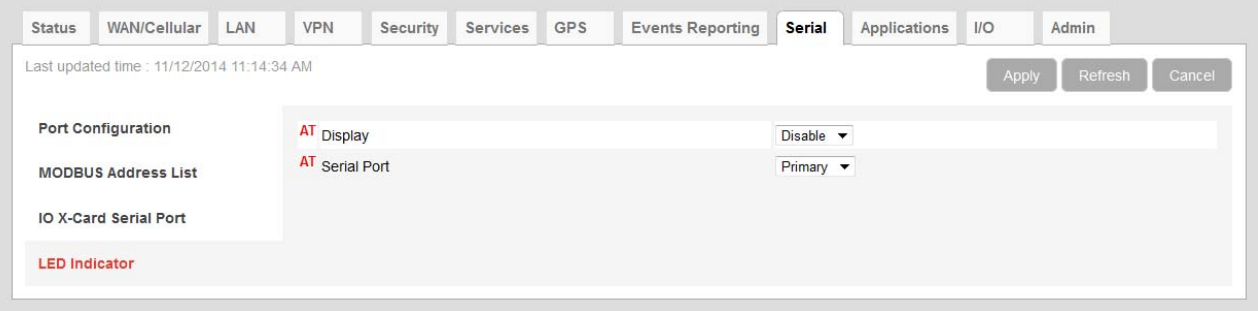


Figure 11-16: ACEmanager: Serial > LED Indicator

Table 11-11: Serial > LED Indicator

Field	Description
Display	Options are: • Disable (default) • Enable If this field is set to Enable, the Activity LED on the AirLink device flashes red when traffic is being transmitted/received on the serial port selected in the Serial Port field. **Activity LED** / **Traffic** Off / No traffic Flashing Green / Traffic on WAN interface Flashing Red / Traffic on selected serial port Flashing Yellow / Traffic on both the WAN interface and selected serial port You can also use an AT command to configure this field. See *SERIALLEDDISPLAY on page 434. For a complete list of LED behavior, refer to the AirLink device Hardware User Guide.
Serial Port	If you have an AirLink GX device with an I/O X-Card installed, use this field to select the serial port you want the LED to indicate traffic on. • Primary—Serial port on the AirLink device itself (default) • X-Card—Serial port on the I/O X-Card installed on the AirLink GX Series device For all other AirLink devices, leave this field set to the default value. You can also use an AT command to configure this field. See *SERIALLEDPORT on page 434.

12: Applications Configuration

The Applications tab consists of a Data Usage section, a Garmin application, and an ALEOS Application Framework section.

Data Usage

Note: Before configuring Data Usage, ensure that the AirLink device receives date and time information from the cellular network, or from GPS in the case of GX Series or LS300 devices using GPS. You can also use the ACEmanager SNTP client to receive time from an SNTP server. (See Time (SNTP) on page 225.) If necessary, contact your Mobile Network Operator to confirm that the cellular network provides date and time information to connected devices.

The Data Usage feature on the Applications tab in conjunction with Events Reporting provides you with a way to actively monitor cellular data usage.

Once data usage is configured, you can use event reporting to:

- Actively monitor the cellular data usage by configuring monthly and/or daily usage level thresholds that result in notifications being sent to you (e.g. email, SMS, or SNMP Trap) when the threshold is reached.
- Limit mobile network communication until the end of the billing period when the data limit is reached by blocking connected LAN devices from using the mobile network. Traffic sent to and from the AirLink device is not blocked. Over-the-air access to ACEmanager and the Telnet/SSH AT interface is still available.

Note: You can configure Events Reporting to notify you when the threshold set in Data Usage is reached, but ALEOS does not block further access to the mobile network, unless you also create a second action to Turn Off Services.

Note: ALEOS Data Usage is approximate and should not be compared with data usage recorded by the Mobile Network Operator.
Sierra Wireless is NOT responsible for data overages.

Step 1—Configure Data Usage

1. In ACEmanager, go to Applications > Data Usage.
2. In the Usage Monitoring field, select Enable.
3. Enter the desired values in the Daily or Monthly Limit fields (in GB or MB), and the day of the month that the billing cycle starts. For more details, see the table starting on page 304.
4. Click Apply.

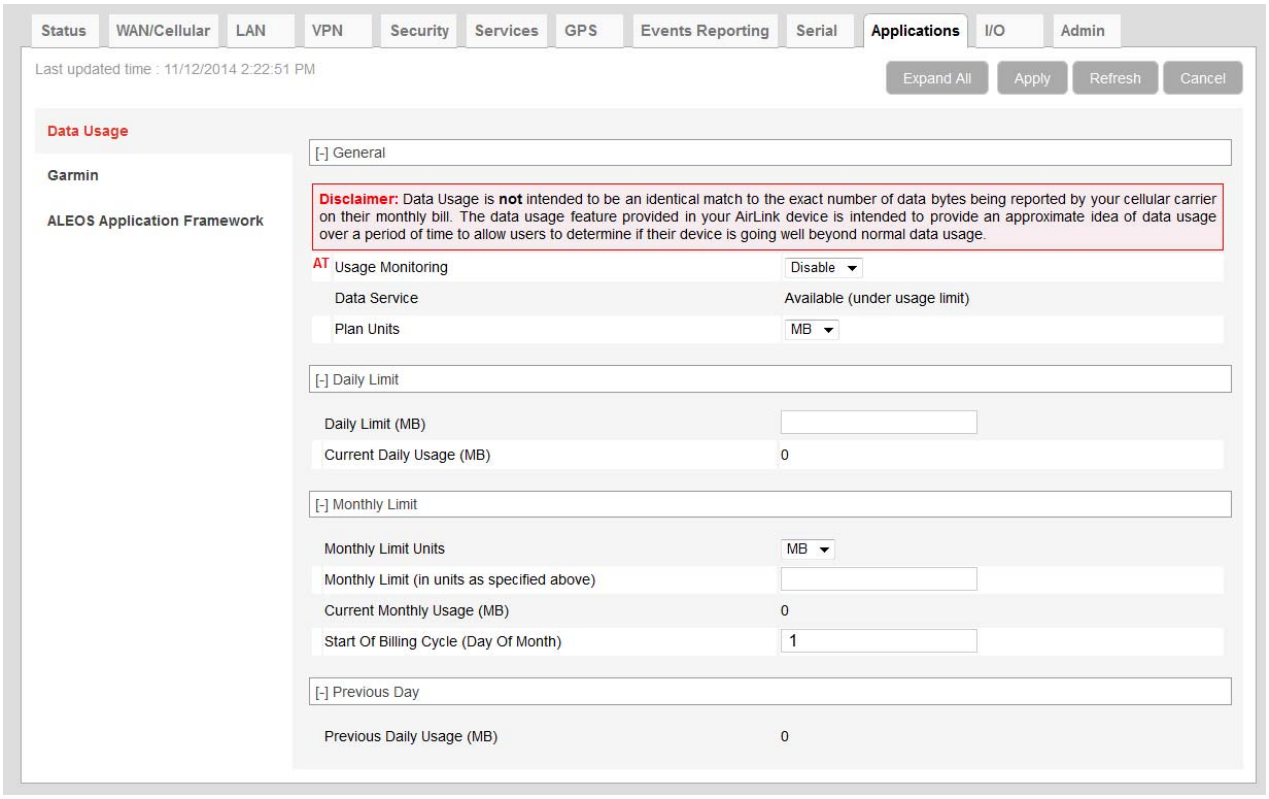


Figure 12-1: ACEmanager: Applications > Data Usage

Field	Description
General	
Usage Monitoring	Use this field to enable or disable data usage monitoring. Options are: • Disable (default) • Enable

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Data Service</td><td>This field is intended for use in conjunction with Events Reporting, specifically a Data Usage Event with Turn Off Services as the configured action. For more information and instructions on configuring the appropriate Event Reporting settings, see Stopping Service when the Event Reporting Threshold is Reached on page 310.
<table>
<tr><th>Data Usage</th><th>Turn Off Services Events Reporting action configured</th><th>Data Service displays....</th></tr>
<tr><td>Over threshold configured in Events Reporting</td><td>No</td><td>Available (under usage limit)</td></tr>
<tr><td>Under threshold configured in Events Reporting</td><td>Yes</td><td>Available (under usage limit)</td></tr>
<tr><td>Over threshold configured in Events Reporting</td><td>Yes</td><td>Blocked (usage limit exceeded)</td></tr>
</table>
Warning: This field shows the status of the data usage, but mobile network access is not actually stopped when this field reads “Blocked (usage limit exceeded” unless you have also configured Event Reporting to Turn Off Services when the threshold is reached. See Stopping Service when the Event Reporting Threshold is Reached on page 310.</td></tr>
<tr><td>Plan Units</td><td>Select the units used for your data plan. The options are:
MB—Megabytes (default)
KB—Kilobytes
Note: When you change the units in this field, the units for values in the Daily Limit and Monthly Limit fields are not converted and must be updated manually.</td></tr>
</table>

Field	Description
Daily Limit	
Daily Limit (MB) **Daily Limit (KB)**	This is the user-specified daily (24 hour) data usage limit (in MB or KB, depending on the value in the Plan Units field). You can specify data usage limits on a daily basis. A limit is essentially a threshold that can trigger the software to take a user-specified action if the usage goes above the threshold. See Events Reporting Configuration on page 257. *Note: The Daily Limit value MUST be expressed as an integer (i.e., a whole number) and NOT as a fraction (e.g., "3.5").* *Note: Daily usage is cleared at midnight, UTC.* **Caution:** *Data usage limits are approximate and based on reporting conditions in ALEOS. Data usage may run over the amount set in this field before the action specified for the threshold trigger takes effect.* **Tip:** *ALEOS reads the data usage every 3 to 5 minutes. If you are using an application that requires high data usage, you can set an alert to warn you when data usage reaches a safe limit that takes into account the amount of data expected over the 3 to 5 minutes between data usage readings. For information on how to set an alert or other action, see Events Reporting Configuration on page 257.*
Current Daily Usage (MB) **Current Daily Usage (KB)**	Displays the current daily data usage (in MB or KB, depending on the option selected in the Plan Units field) *Note: Data usage includes data sent and data received.*

Field	Description
Monthly Limit	
Monthly Limit Units	Select the units for monthly data usage—MB (default) or GB. This field only appears when Plan Units on page 305 is set to MB.
Monthly Limit (in units as specified above)	This is the user-specified monthly data usage limit (in MB or GB, depending on the option selected in Monthly Limit Units). Data usage accumulates on a monthly basis and on the date you specified (the "rolling month"). Data usage accumulates during the month until the end of the next billing period, at which point the data usage totals are reset. *Note: The Monthly Limit value MUST be expressed as an integer (i.e., a whole number) and NOT as a fraction (e.g., "3.5")* *Note: Monthly usage is cleared at midnight, UTC on the last day of the billing cycle.* **Caution:** *Data usage limits are approximate and based on reporting conditions in ALEOS. Data usage may run over the amount set in this field before the action specified for the threshold trigger takes effect.*
Current Monthly Usage (MB) **Current Monthly Usage (KB)**	Displays the current monthly data usage (in MB or KB, depending on the value configured in Plan Units on page 305.) *Note: Data usage includes data sent and data received.*
Start of Billing Cycle (Day of Month)	Enter the desired start of the billing cycle. For example, 3 (Day 3 of every month) Changing the value in this field resets the Current Monthly Usage (MB) field to zero.
Previous Day	
Previous Daily Usage (MB) **Previous Daily Usage (KB)**	Shows the data usage for the previous day (in MB or KB, depending on the value configured in Plan Units on page 305.) *Note: Data usage includes data sent and data received.*

Step 2—Configure Event Reporting

1. In ACEmanager, go to Events Reporting > Actions.

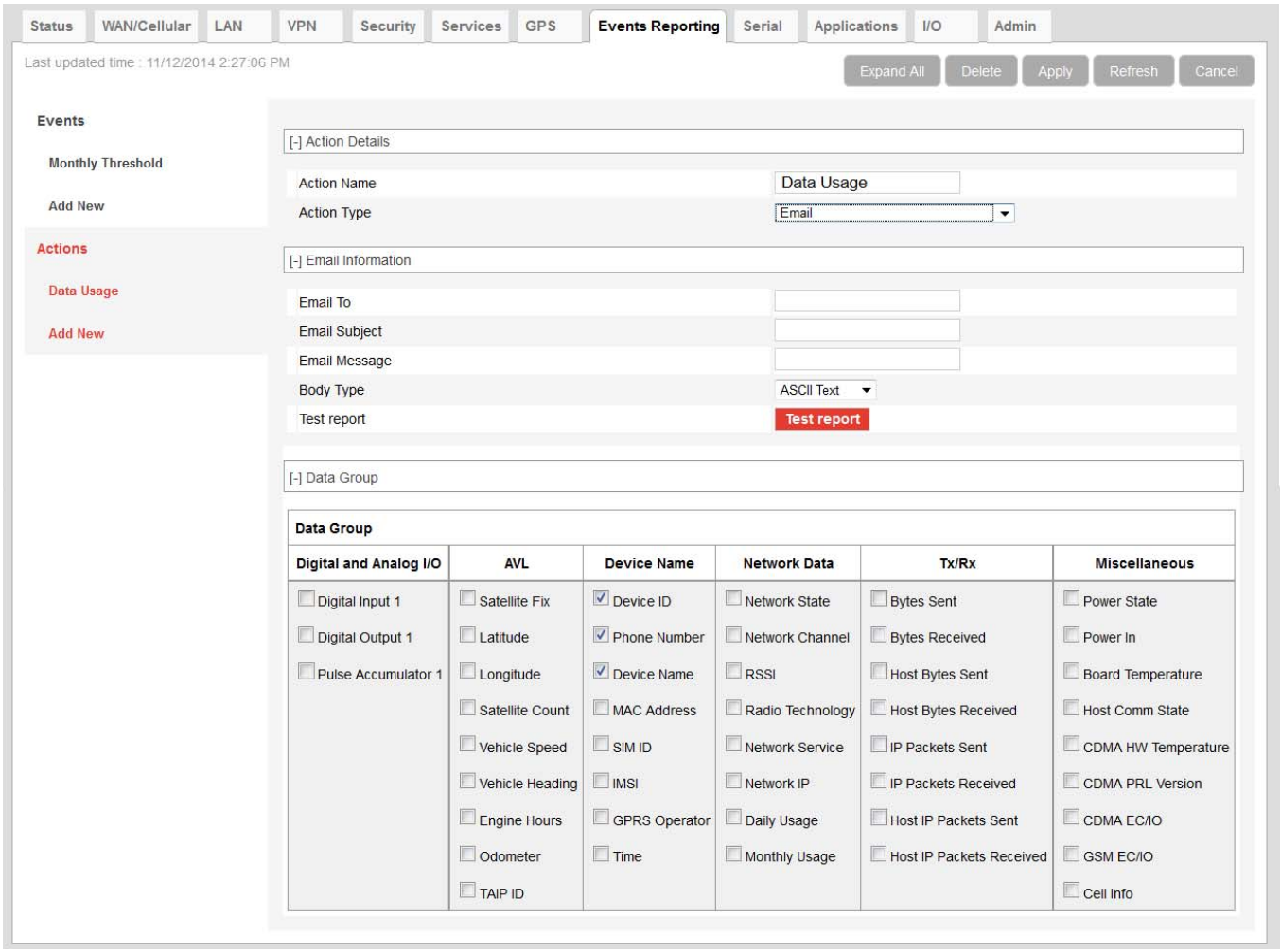
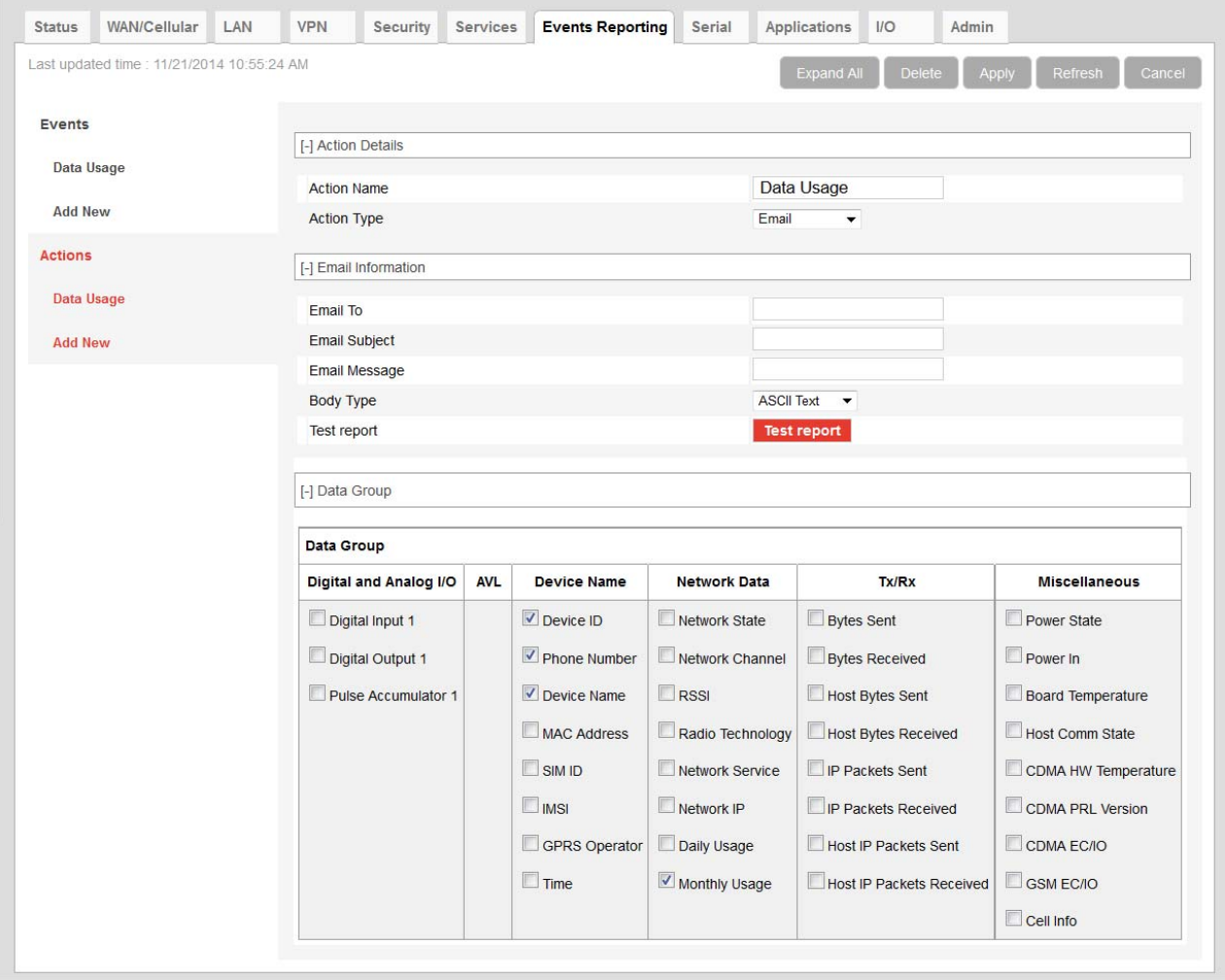


Figure 12-2: ACEmanager: Events Reporting > Actions



2. Select the desired Action to be performed when the Event is triggered, such as SNMP Trap or Email, and enter the appropriate information in the related fields. For detailed instructions, see Configuring Events Reporting on page 258.
3. If you selected Email or SMS, select the check box(es) in the Data Group section of the screen to indicate the information to be included in the email or SMS.

Note: You can have more than one Action for a single Event, but you can only have one Daily Usage and one Monthly Usage Event.

4. Click Apply.
5. Go to Events Reporting > Events and configure a data usage threshold.

   The threshold is specified as a percentage of the monthly or daily limit. For example, if you have a monthly limit of 5 GB, and the threshold is set at 80%, then threshold is reached at 4 GB of data. For detailed instructions, see Configuring Events Reporting on page 258.

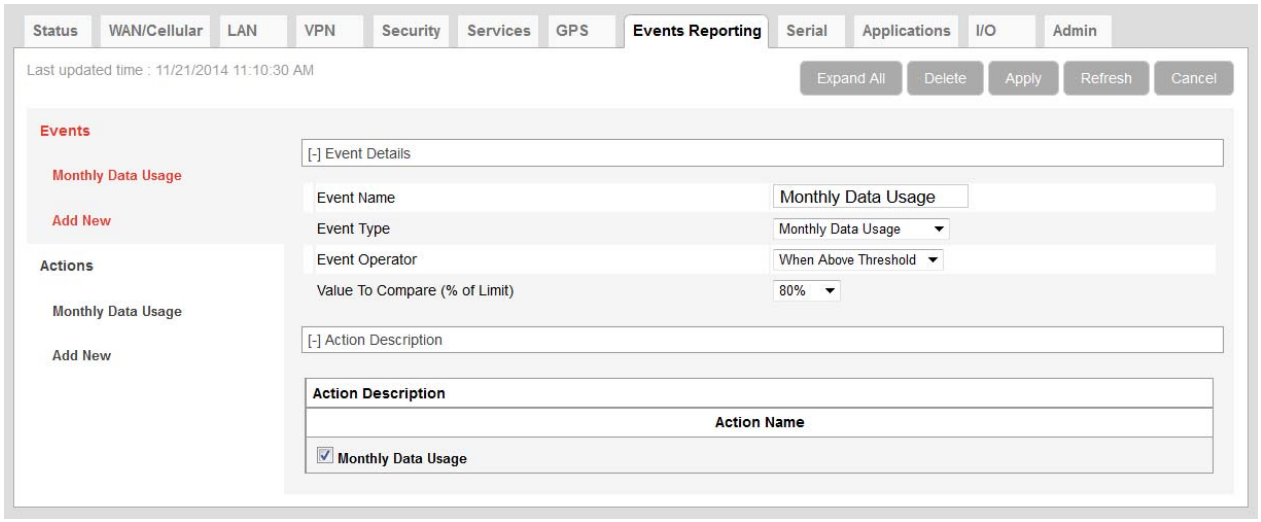


Figure 12-3: ACEmanager: Events Reporting > Events

6. At the bottom of the screen, select the check box beside the Action you want to associate the Event with.
7. Click Apply.

Stopping Service when the Event Reporting Threshold is Reached

When you are approaching the data plan limit, you may want to turn off cellular communication to any connected user devices until the next billing cycle starts.

To turn off services on the data plan when the limit is reached:

1. In ACEmanager, go to Events Reporting and select Actions Add New on the left menu.
2. Enter the desired name for the action.
3. In the Action Type field, select Turn Off Services.

   When triggered, this action prevents cellular communication to all connected devices. Traffic sent from the AirLink device is not blocked. Over-the-air access to ACEmanager and the Telnet/SSH AT interface is still available.

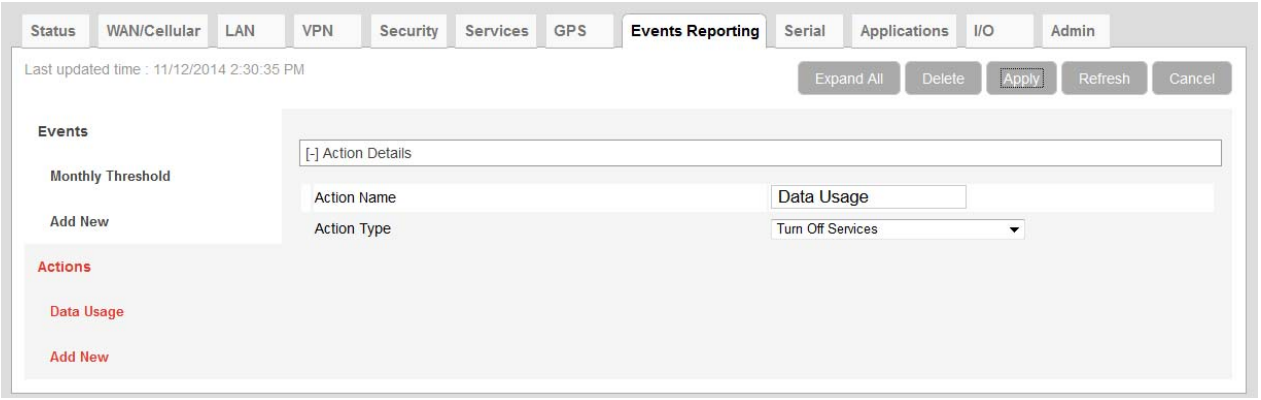


Figure 12-4: ACEmanager: Events Reporting

4. Click Apply.
5. Select Events on the left menu.
6. Enter the desired Event Name.
7. In the Event Type field, select either Daily Data Usage or Monthly Data Usage.
8. In the Event Operator field, select When Above Threshold.
9. Set the desired Value to Compare (% of limit).
10. At the bottom of the screen, select the check box beside the Action you want to associate the Event with.

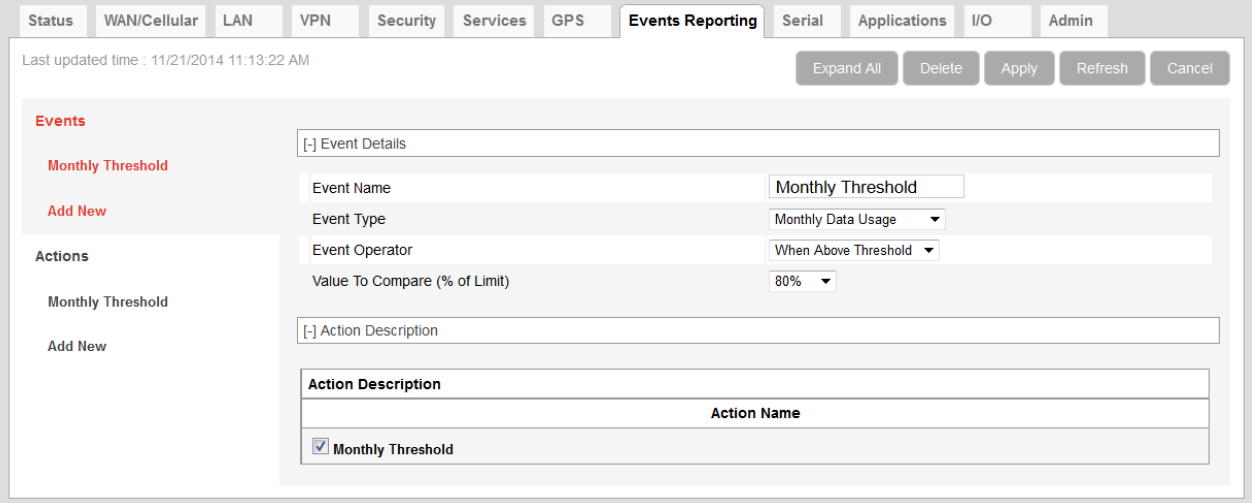


Figure 12-5: ACEmanager: Events Reporting > New Event

11. Click Apply.

Note: When the configured threshold is crossed, all traffic between connected devices and the network is blocked. This helps to reduce data usage, but it does not completely stop it. Traffic to and from the AirLink device is not blocked, and over-the-air access to ACEmanager and the Telnet/SSH AT interface is still available.
Setting the "Turn Off Services" threshold at a level below 100% of the data plan helps to reduce data usage before the data plan limits are exceeded.

Garmin

Garmin provides navigation devices for versatile fleet monitoring solutions. AirLink devices provide Internet access to Garmin devices and a mechanism to enable via cellular. ALEOS also monitors links to the Garmin device and communication between the Garmin device and the server.

To configure Garmin in ACEmanager:

1. Under the Applications > Garmin, set the Garmin Device Attached feature to Enabled.

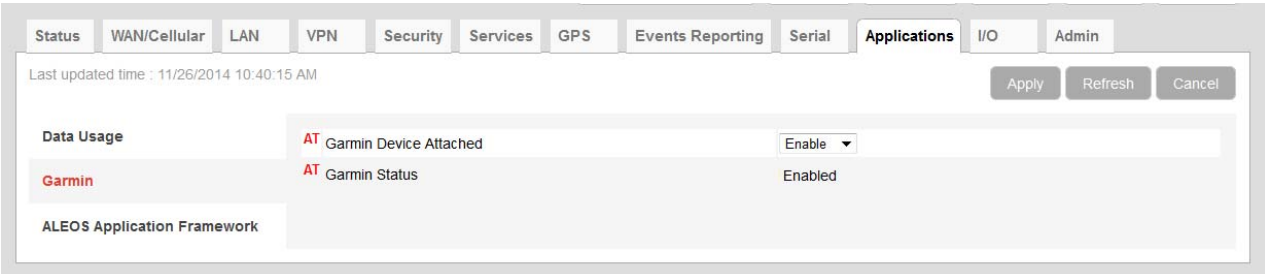


Figure 12-6: ACEmanager: Applications > Garmin

2. Go to Serial > Port Configuration.
   - Set the Startup Mode Default field to TCP.
   - Set the Server Address and Port for TCP.
   - Set the Destination Port and the Destination Address to the port and address of the AVL server that the TCP application will be communicating with.
3. Configure the serial port. To communicate with Garmin:
   - Input **9600, 8N1** in Configure Serial Port
   - Select **None** in Flow Control
   - Select **Ignore DTR** in DTR Mode.

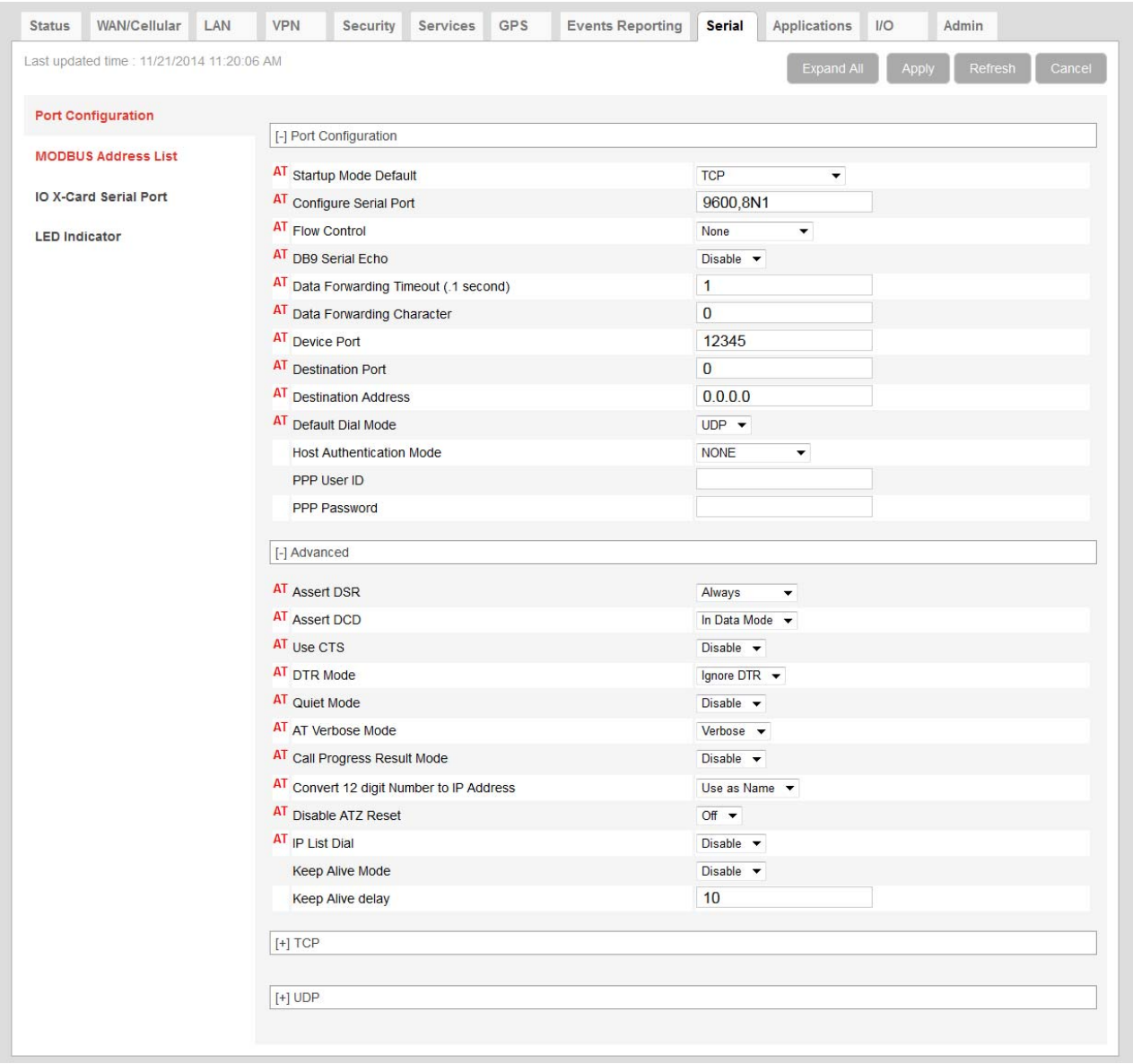


Figure 12-7: ACEmanager: Serial > Port Configuration

Check the Garmin's communications status under the Status > Applications tab. Garmin data service states are:

- Not Enabled — Not acknowledged by the AVL server
- Enabled — Acknowledged by the AVL server.

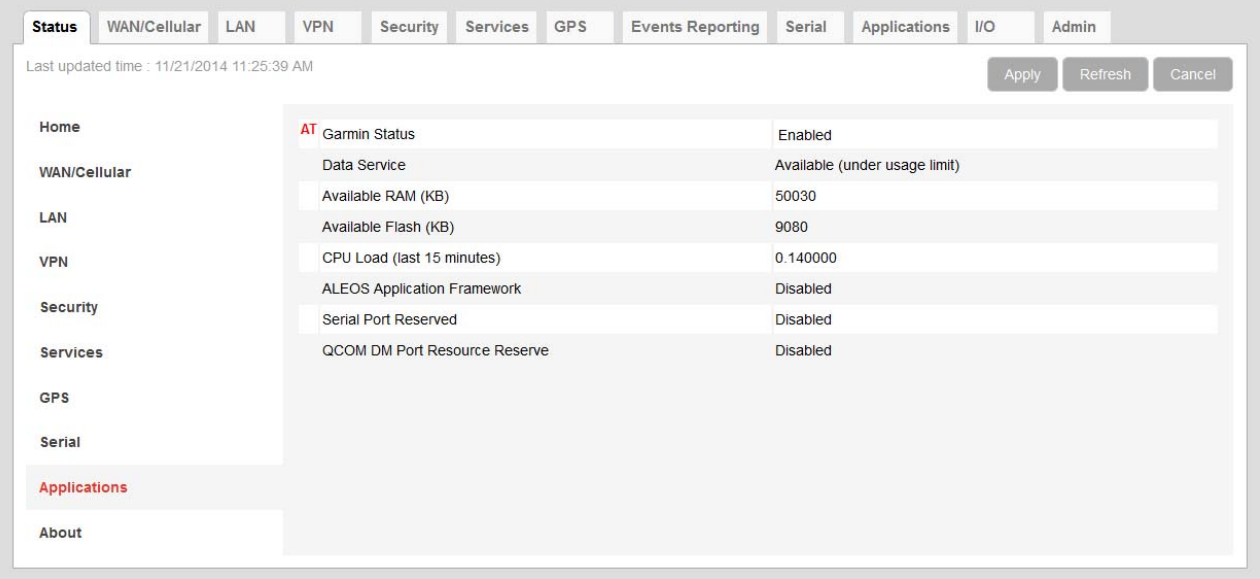


Figure 12-8: ACEmanager: Status > Applications > Garmin Status

4. Reboot the AirLink device to apply the changes. The “Garmin Status” now appears:
   - Enabled — Acknowledged by the AVL server.

*Note: The Garmin Status field appears **only** if the Garmin application is Connected.*

ALEOS Application Framework

ALEOS Application Framework (ALEOS AF) allows you to develop your own applications to run inside an AirLink device and leverage the AirVantage M2M Cloud Platform (www.sierrawireless.com/AirVantage) or a customer-developed server platform. Embedded and server application developers can start using ALEOS AF by accessing the Sierra Wireless Developer Zone (http://developer.sierrawireless.com/ALEOS_AF).

You may want to reserve the serial port for an ALEOS AF application. To do so, select Enable in Applications > ALEOS Application Framework > Serial Port Reserved.

It is not necessary to reserve the serial port before activating ALEOS AF.

Reserving the serial port is mandatory only if the ALEOS AF application will be using the serial port.

Note: When you reserve the serial port for ALEOS AF, it cannot be used for any other serial-related ALEOS features.

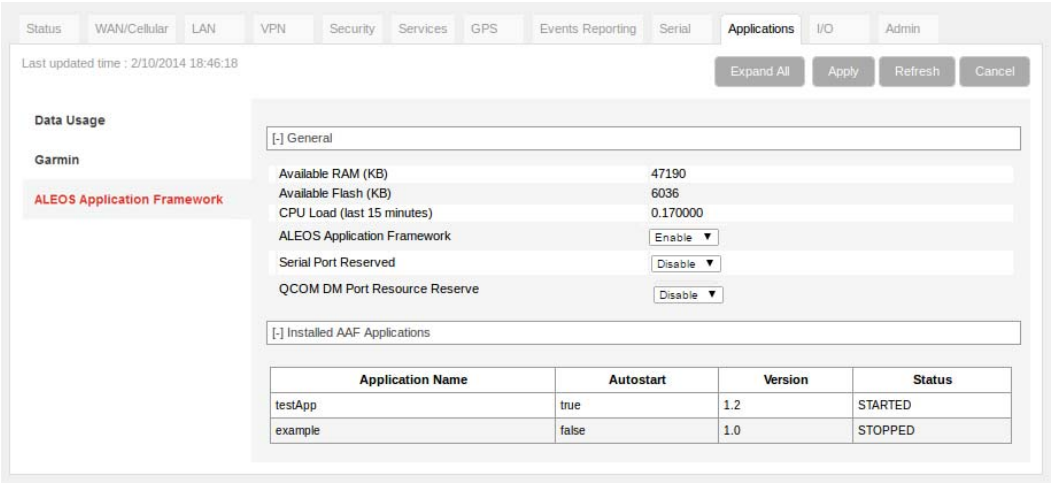


Figure 12-9: ACEmanager: Applications > ALEOS Application Framework

Field	Description
General	
Available RAM (KB)	Available RAM in kilobytes (1000 bytes), updated every 30 seconds
Available Flash (KB)	Available Flash on the user partition in kilobytes (1024 bytes), updated every 30 seconds
CPU Load (Last 15 minutes)	CPU load, averaged over the last 15 minutes and updated every 30 seconds The CPU load relates to how many applications are attempting to execute in parallel over the 15-minute period. If the load is greater than 1, some applications are waiting for CPU capacity to become available and may be delayed in launching.
ALEOS Application Framework	Enable or disable (default) the ALEOS Application Framework (ALEOS AF). If enabled, ALEOS AF starts at boot time. When the Reset to Factory default button on the Admin > Advanced page is pressed, ALEOS AF is disabled.
Serial Port Reserved	Select Enable to reserve the serial port for ALEOS AF. When this field is set to Enable, the serial port cannot be used for any other serial-related ALEOS features. The options are: • Disable (default) • Enable
I/O X-Card Serial Port Reserved	This field only appears on a GX Series device with an I/O X-Card installed. Select Enable to reserve the serial port on the I/O X-Card for ALEOS AF. When this field is set to Enable, the serial port cannot be used for any other serial-related ALEOS features. The options are: • Disable (default) • Enable
QCOM DM Port Resource Reserve	Reserves the QCOM DM port for ALEOS AF applications. Options are: Enable (Reserve access for ALEOS AF) or Disable (Reserve access for ALEOS). Default: Disable

Field	Description
Installed AAF Applications	
Application Name **Autostart** **Version** **Status**	To help you manage installed applications, the table in this section shows all the installed AAF Applications and displays the: • Application name • Autostart—true or false • Version • Status—STARTED or STOPPED If no applications are installed, the table displays the message: “No application installed or AAF not started”.

13: I/O Configuration

13

The I/O tab in ACEmanager applies to all Sierra Wireless AirLink devices that feature I/O ports.

You can use the input/outputs on AirLink devices to generate reports based on a threshold being crossed, a switch being opened or closed, or the number of times a switch has changed state.

Use the Events Reporting screen to configure reports. (See Events Reporting Configuration on page 257.) Use the I/O screen to view the current state of the analog and digital inputs, to turn the relays on and off, and to configure the units you want used in the reports based on analog inputs.

The number of digital and analog input/outputs depends on the device and in the case of the AirLink GX, whether or not it has an I/O X-Card installed.

AirLink GX Series device

The AirLink GX Series device without an I/O X-Card installed:

- Has one pin (Pin 4 on the power connector) that can be configured as a digital input/output or a relay output
- Does not support analog input

The AirLink GX Series device with the I/O X-Card installed has:

- Five digital inputs or five relay outputs (configurable)
- Four analog inputs

AirLink LS300

The AirLink LS300 has:

- One pin (Pin 4 on the power connector) that can be configured as a digital input/output, relay output, or analog input.

More information

For more information, refer to the Hardware Configuration User Guide for your AirLink device.

Analog inputs

Analog inputs monitor a voltage range in small increments. This allows you to monitor equipment that reports status as an analog voltage. Examples include:

- Power supply voltage

- Temperature, weight, volume, flow represented as voltage
- An incremental gauge with a voltage output
- Vehicle battery voltage

The raw data for the changes being monitored is in volts, but you can use the I/O Configuration screen in ACEmanager to convert voltage to the desired units of measurement. See Transformed Analog on page 322.

Digital inputs

Digital inputs monitor contact closures on a switch. This allows you to monitor changes such as:

- When a door or latch is open or closed
- When a container is full or empty
- When a switch or valve is opened or closed
- The level of fuel in a vehicle (connected to an on/off sensor)
- When the trunk of a vehicle is opened or closed

You can use Events Reporting to generate reports and actions based on the digital input values.

Volts	Interpreted as
-0.5 – 1.2	Digital 0
2.2 – 30	Digital 1

For more information on setting up reports, see Events Reporting Configuration on page 257.

Relay outputs

You can use relay outputs to trigger an intermediary switch and change the state of equipment.

Current State

The Current State screen allows you to view the current values (as of the last refresh) of analog and digital inputs, pulse counts for digital inputs, and raw and transformed values for analog inputs. You can also use this screen to change the current values for Relay outputs. This change occurs immediately without a reboot.

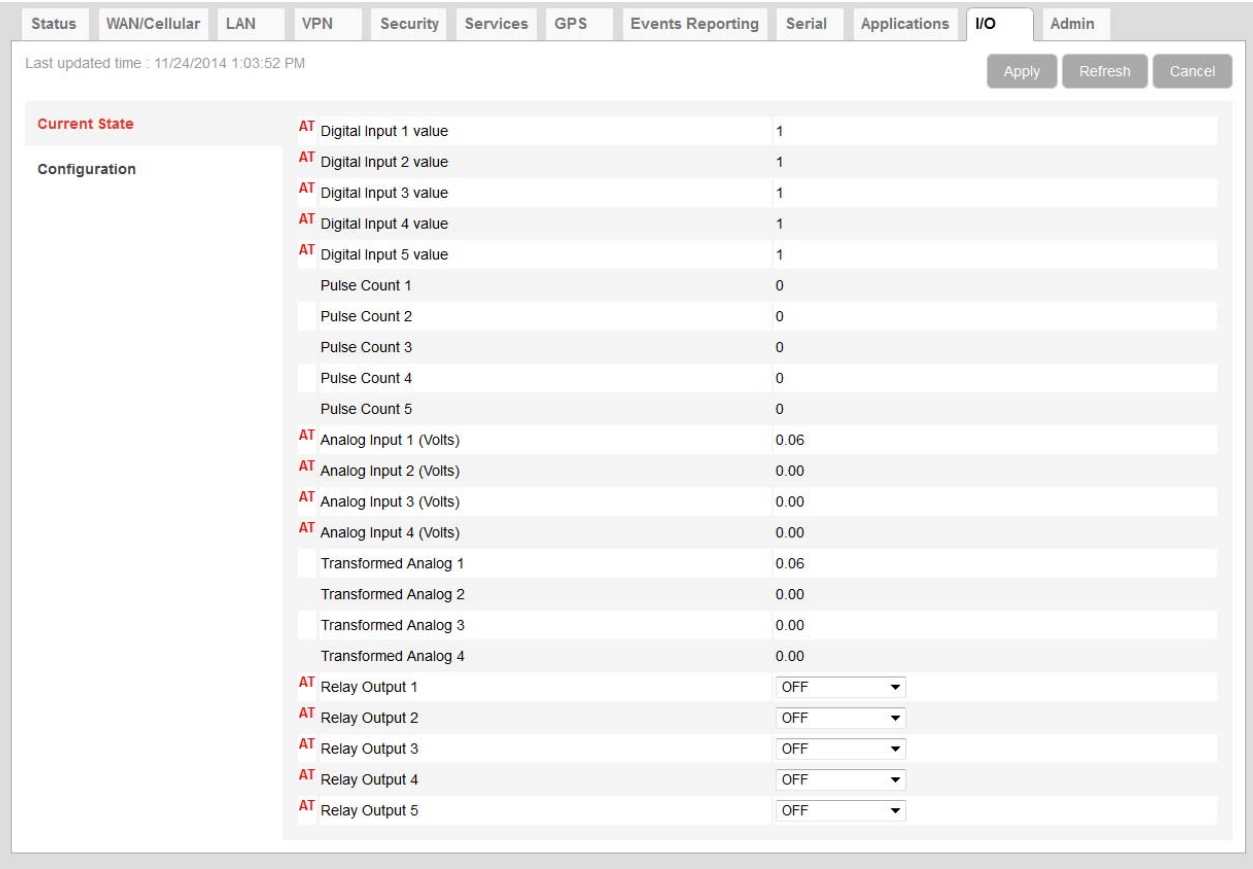


Figure 13-1: ACEmanager: I/0 > Current State (GX Series device with I/O X-Card)

Table 13-1: I/O: Current State

Command	Description
Digital Input # value	Displays the current value for the digital input: • 0 —Open • 1 —Closed Digital input 1 displays the value for Pin 4 on power connector. *Note: Digital inputs 2–5 are only available on an AirLink GX Series device with an I/O X-Card. For pinout details, refer to the GX Series Hardware User Guide.* You can also use an AT command to read these values. See *DIGITALIN[n]? on page 442.

Table 13-1: I/O: Current State

Command	Description
Pulse Count #	The pulse count increments when the input value changes from high to low. Pulse count 1 displays the value for Pin 4 on power connector. *Note: Pulse counts 2–5 are only available on an AirLink GX Series device with an I/O X-Card. For pinout details, refer to the GX Series Hardware User Guide.* *Note: To reset the pulse count to zero, reset the device to the factory defaults.*
Analog Input # (Volts)	Shows the current state of individual analog inputs The analog inputs report the voltage in volts. Range is 0–30 volts. You can also use an AT command to read these values. See *ANALOGIN[n]? on page 442.
Transformed Analog #	Shows the individual analog inputs in the units configured on the I/O Configuration screen
Relay Output #	Configure Relay Output signal. Options are: • OFF (default) The circuit is open. • Drive Action Low—equivalent to ON. The circuit is closed. Relay output 1 displays the value for Pin 4 on power connector. *Note: Relay outputs 2–5 are only available on an AirLink GX Series device with an I/O X-Card. For pinout details, refer to the GX Series Hardware User Guide.* *Note: If the same pin can be used for input or output, be aware that changing the output setting could change the input values. For pinout information for your AirLink device, refer to the applicable AirLink product user guide.* You can also use an AT command (see *RELAYOUT[#] on page 442), an SMS command (see [prefix]relay x y on page 448), or a RAP command (refer to the Remote Application Protocol User Guide) to configure this field. *Note: Changes to the relay outputs go into effect immediately. No reboot of the AirLink device is necessary.*

Pulse Count

Pulse Count details:

- Pulses are counted on falling edge (high to low).
- Repeated pulses cannot be counted when the device is powered off, or being reset. However, a single change in state while the device is powered off or being reset is counted properly.
- To reset the pulse count to zero, reset the device to the factory defaults.

Configuration

This screen allows you to configure the initial relay settings and to transform units of measurement for the analog inputs from volts to a more appropriate unit, if applicable. Generated reports use the transformed value configured on this screen.

For more information, refer to the Hardware Configuration User Guide for your AirLink device.

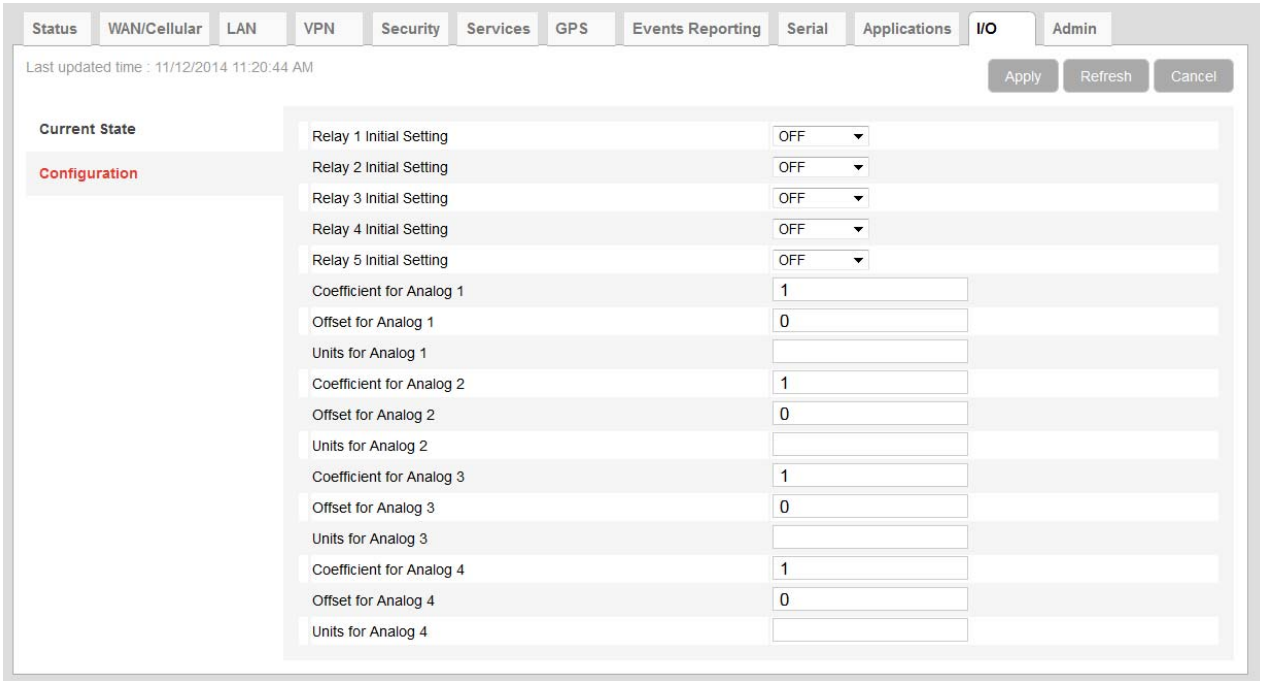


Figure 13-2: ACEmanager: I/O > Configuration

Field	Description
Relay # Initial Setting	The initial relay value when the AirLink device is powered on Options are: • ON • OFF (default) • Last Value (The value remains the same as it was before the AirLink device was powered down). When you change this field, the corresponding digital input value on this screen reflects the change after a screen refresh. Relay 1 Initial Setting displays the value for Pin 4 on power connector. *Note: The Relay 2–5 Initial Setting fields are only available on an AirLink GX Series device with an I/O X-Card. For pinout details, refer to the GX Series Hardware User Guide.*
Coefficient for Analog #	This value may be found in the user guide for the equipment you want to monitor, or you can calculate it from information in the user guide. If this information is not available in the documentation that came with the equipment you want to monitor, contact the manufacturer. For an example of how to calculate the coefficient, see Transformed Analog on page 322.
Offset for Analog #	The offset (difference) between 0 volts and the equivalent value for the desired unit of measurement
Units for Analog #	The unit of measurement used in event reporting for the parameter being monitored by the analog input For example: degrees Celsius, degrees Fahrenheit, liters, mm, etc.

Transformed Analog

The raw analog data is displayed in volts. However, that is not always the most convenient unit of measurement to view the data. The I/O Configuration screen enables you to transform the voltage readings to a more convenient unit of measurement, for example degrees Celsius or Fahrenheit for temperature, liters for volume, etc.

Step 1—Coefficient and Offset

Before you configure ACEmanager, you need to locate or calculate the coefficient and the offset values.

Consult the user documentation for the equipment you want to monitor. It should provide you with the coefficient to convert volts to the appropriate unit of measurement and the offset value (the difference between the equivalent value for 0 volts and 0), or provide information on equivalent values for voltage readings from which you can calculate the coefficient and offset. (If this information is not available in the user documentation, contact the manufacturer.)

For example, if the equipment monitors temperature, and has a scale from 0 volts to 30 volts, the equipment specifications should provide information similar to the following:

0 V is equivalent to - 20°C

30 V is equivalent to 100°C

This is expressed algebraically as follows:

$$a \times 0V + b = -20C$$

$$a \times 30V + b = 100C$$

where:

a = coefficient

b = offset

For this example, you can calculate a as follows:

$$(a \times 30V + b) - (a \times 0V + b) = 100C - (-20)$$

$$a \times 30V = 120V$$

$$a = 4$$

To calculate b, substitute a into the first equation above:

$$4 \times 0V + b = -20$$

$$b = -20$$

Step 2—Configure ACEmanager

For each of the analog inputs you want to configure:

1. In ACEmanager, go to I/O > Configuration.
2. Enter the values for the coefficient and offset. (In this example, the coefficient is 4 and the offset is -20.)
3. Enter the desired unit of measurement. (In this example, the unit of measurement is C, for degrees Celsius).

ACEmanager shows the value of the transformed analog input as temperature in C.

Note: A reboot is required after configuring the transformed analog values.

Change Password

For system security reasons, changing the default password of the AirLink device is highly recommended.

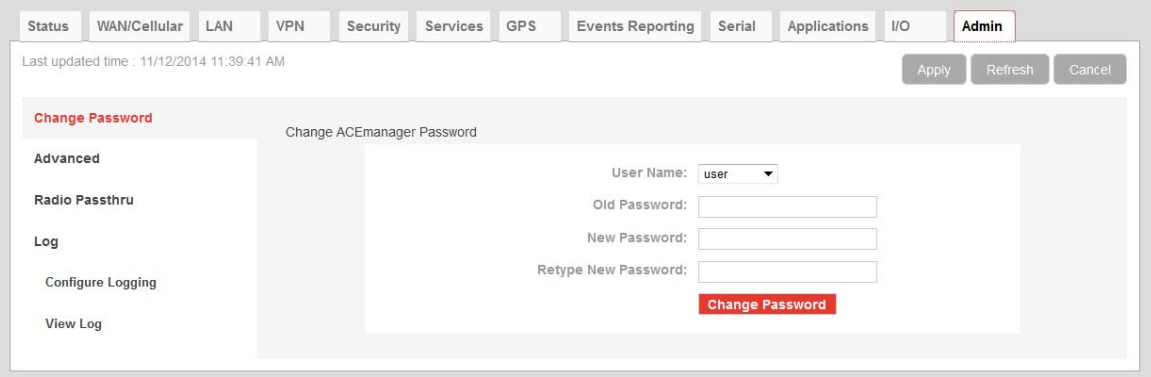


Figure 14-1: ACEmanager: Admin

To change the default password:

1. Select the User Name associated with the password you want to change: user, viewer, or sconsole.
2. Enter the old password.
3. Enter the new password twice.

   The password can be 4 to 32 characters long and can contain a mixture of letters, numbers, and/or special characters. The password is case sensitive.
4. Click Change Password.

If you want to confirm that the password has been changed, log out and then log in with the new password.

Note: There are two user levels in the User Name drop-down menu. The 'user' has full administrator rights and can edit the configuration; the 'viewer' can only view the configuration and status of the device. Viewer can change the 'viewer' password. User can change both.

Advanced

Features which should be rarely changed and will affect the operation of the device are present on the Advanced screen.

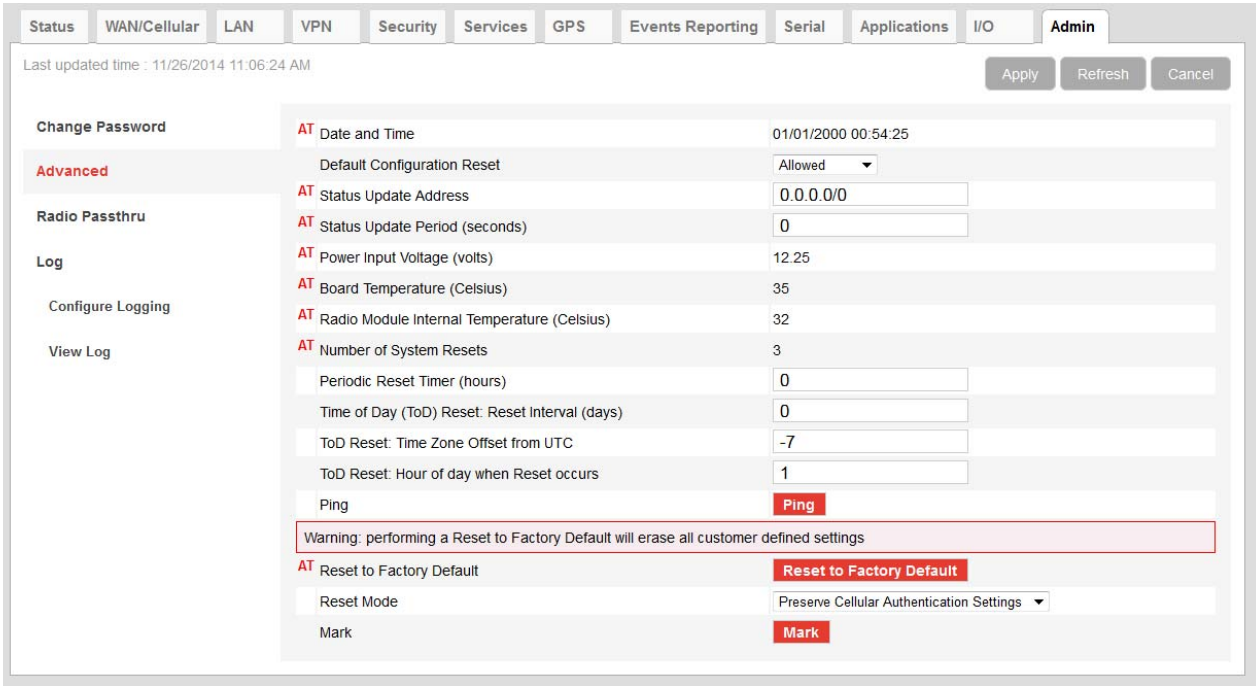
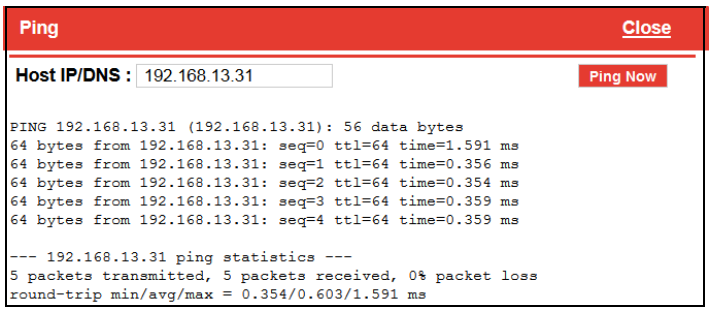
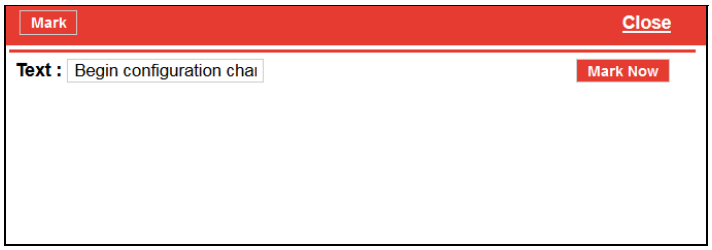


Figure 14-2: ACEmanager: Admin > Advanced

Field	Description
Date and Time	Queries the internal clock. The date and time are always specified in 24-hour notation (UTC). • mm/dd/yyyy= date in month/day/year notation • hh:mm:ss= time in 24-hour notation
Over-the-Air Programming	Enables/disables over-the-air ALEOS software upgrading of the AirLink device. When Sierra Wireless releases a new version of ALEOS, you can upgrade your remote devices with Over-the-Air Programming (OPRG) enabled. • Enable (default) • Disable
Default Configuration Reset	Enables or disables the hardware reset button Sets the AirLink device to allow (or not allow) the hardware reset button to reset the device to the factory default settings. • Allowed—Pressing the hardware reset button for 7–10 seconds reboots the device and resets it to the factory defaults. (When resetting the device to factory default settings, release the reset when all four LEDs turn from red to yellow.) • Not Allowed—Pressing the hardware reset button reboots the device, but does **not** reset it to the factory defaults. *Note: You can always use the "Reset to Factory Defaults" button in ACEmanager to reset the device. This field only affects the **hardware** reset button on the device.*

Field	Description
Status Update Address	Enter the device Name/Port. Name is the domain name or IP address, and Port is the port of the device where the device status updates will be sent. This report can be sent to a LAN connected host (e.g., 192.168.13.100/1122) or a remote location (e.g., newb.eairlink.com/17000). The status parameters are sent in an XML format.
Status Update Period (seconds)	The time interval (in seconds) when a status update should be sent
Power Input Voltage (volts)	Displays the power input voltage in volts. If the input voltage ground is connected to the AirLink device case (without serial connection), this value reads .3 V (approx.) less; if ground is connected (with serial connection), the value reads .3 V (approx.) more.
Board Temperature (Celsius)	Displays the board temperature in degrees (Celsius)
Radio Module Internal Temperature (Celsius)	Displays the temperature of the internal radio module in degrees (Celsius).
Number of System Resets	Counter of the number of system resets over the life of the device or since the configuration was reset
Periodic Reset Timer (hours)	Resets the device after the specified number of hours. 0 = disabled
ToD Reset: Reset Interval (days)	Number of days between resets 0 = Disabled Example: If this field is set to 3, the device resets every third day.
ToD Reset: Time Zone Offset from UTC	Time zone adjustment (Offset in easterly direction from UTC Time) Possible values are -12...12 Example: Pacific Standard Time would be -7
ToD Reset: Hour of day when Reset occurs	The local hour of the day when the reset occurs Possible values are 0–23 Example: 4 is 4:00 am
Ping	Use this button to confirm that a connected device is responding. 1. Click Ping. 2. In the pop-up window, enter the device IP address or DNS name and click Ping Now. 
Reset to Factory Default	Erases all customer-defined settings, including custom APNs and resets all settings (passwords, LAN and WAN configuration, security settings, ALEOS Applications Framework, etc.) to the original factory settings. ALEOS AF is also reset to disabled.

Field	Description
Reset Mode	Before resetting the AirLink device to the factory default settings, you can choose to preserve the configured network connection settings. Options are: • Reset All—All settings including network settings are returned to the factory default values on Reset to Factory Default. Note: Custom APNs on AirLink devices with radio module MC7750 retain a custom APN after the reset to factory default settings. To change the APN, go to WAN > Cellular. To determine the type of radio module in your device, go to Status > About. • Preserve Cellular Authentication Settings—(default) When the device is returned to factory default settings (either by clicking the Reset to Factory Defaults button in ACEmanager, or pressing the hardware reset button as described in the Hardware User Guide), the following network settings are preserved: • Network User ID • Network Password • Network Authentication Mode • LTE Authentication Mode • APN Type • Select from the List (APN value) • User Entered AP • Backup APN • Backup Network Authentication Mode • Backup LTE Authentication Mode • Backup Network User ID • Backup Network Password • SIM Card Pin code • Status of the last PIN lock/unlock attempt • AVMS Enabled/Disabled status • AVMS Name (Device name in AVMS) • Device Initiated Interval (AVMS) • AVMS Server URL • Reset Mode

Field	Description
Mark	This button is used to mark the start of a section in the device log and is typically used for troubleshooting. If asked to do so: 1. Click the Mark button and enter the text you want to appear in the log file. Alphanumeric characters, spaces, periods, commas, dashes, colons and semi-colons are allowed.  2. Click Mark Now. 3. Proceed with the configuration changes. 4. Generate a log file. (See Log on page 330.)

Radio Passthru

Radio Passthru allows a direct connection, using USB, to the internal radio. Normal cellular radio operation is suspended while Radio Passthru is enabled.

Radio Passthru is generally used only in certain troubleshooting scenarios.

The hardware bypass will remain in effect until the ALEOS software resets either via ACEmanager command or the hardware Reset button.

Note: Because Radio Passthru is not USB/net or USB/serial, a different set of drivers are required to connect to the radio installed inside an AirLink device. Additionally, while it is possible to send AT commands to the radio using a terminal connection, there are software applications designed to communicate with the radio directly. If you need to use Radio Passthru, contact your Sierra Wireless AirLink representative to obtain the needed drivers and/or software application.

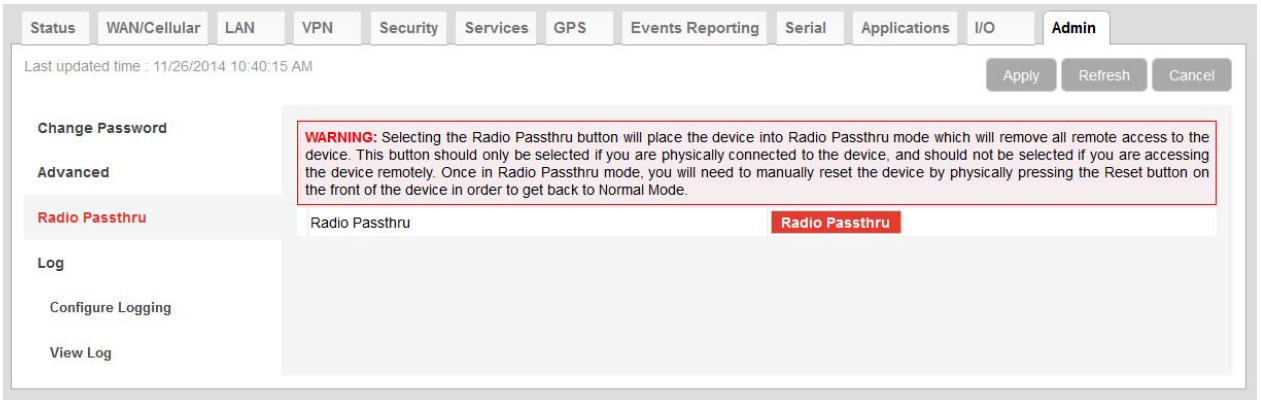

Status
WAN/Cellular
LAN
VPN
Security
Services
GPS
Events Reporting
Serial
Applications
I/O
Admin
Last updated time : 11/26/2014 10:40:15 AM
Apply
Refresh
Cancel
Change Password
Advanced
Radio Passthru
Log
Configure Logging
View Log
WARNING: Selecting the Radio Passthru button will place the device into Radio Passthru mode which will remove all remote access to the device. This button should only be selected if you are physically connected to the device, and should not be selected if you are accessing the device remotely. Once in Radio Passthru mode, you will need to manually reset the device by physically pressing the Reset button on the front of the device in order to get back to Normal Mode.
Radio Passthru
Radio Passthru

Figure 14-3: ACEmanager: Admin > Radio Passthru

Log

The Log file is a system log of the AirLink device.

The Logging configuration screen enables you to configure log verbosity and display filtering. The View Log screen enables you to view and save logs. The logs are in plain text.

To configure what you want to include in the logs:

1. In ACEmanager, go to Admin > Log.

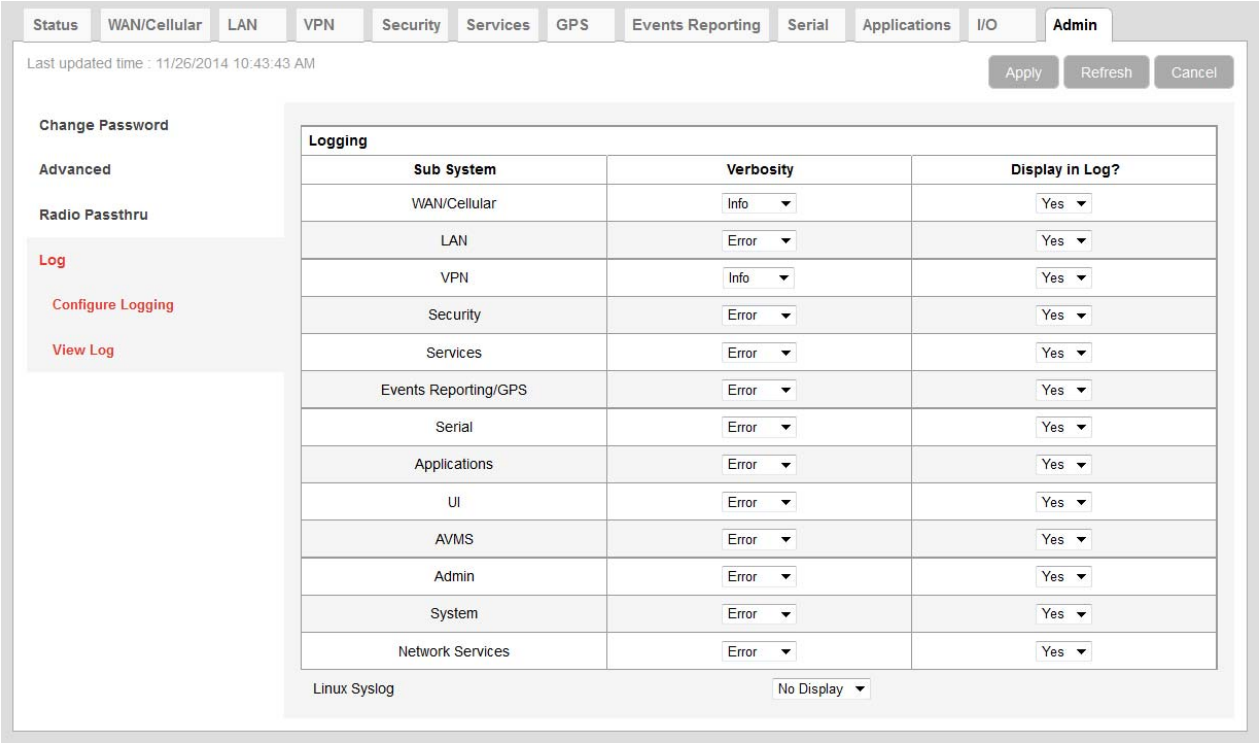


Figure 14-4: ACEmanager: Admin > Log, Configure Logging

2. For each subsystem listed:

   a. Select whether or not to display it in the log.

   Separate filters, based on subsystem and severity, are applied when the messages are generated and when the messages are displayed. Four severity levels are supported for filtering in the drop-down lists for verbosity:

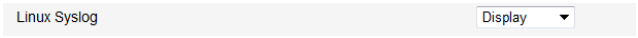
   - Critical
   - Error
   - Info (information)
   - Debug

Note: The VPN Sub System only allows for Info and Debug. For maximum information, set the VPN verbosity to Debug.

   b. Select the verbosity level.

Note: Some log messages are only displayed if you display Linux Syslog. For example, If you are debugging a VPN or LAN setup, the relevant information is only displayed in the Linux Syslog.

3. Optional: To display Linux Syslog:
   a. Ensure that Display (default value) is selected the drop-down menu beside Linux Syslog.



4. Click Apply.
5. If you have changed any of the verbosity levels or the Linux syslog setting:
   a. Reboot the AirLink device.
   b. Log into ACEmanager, go to Admin > Log.
6. Select View Logs from the menu on the left side of the page.

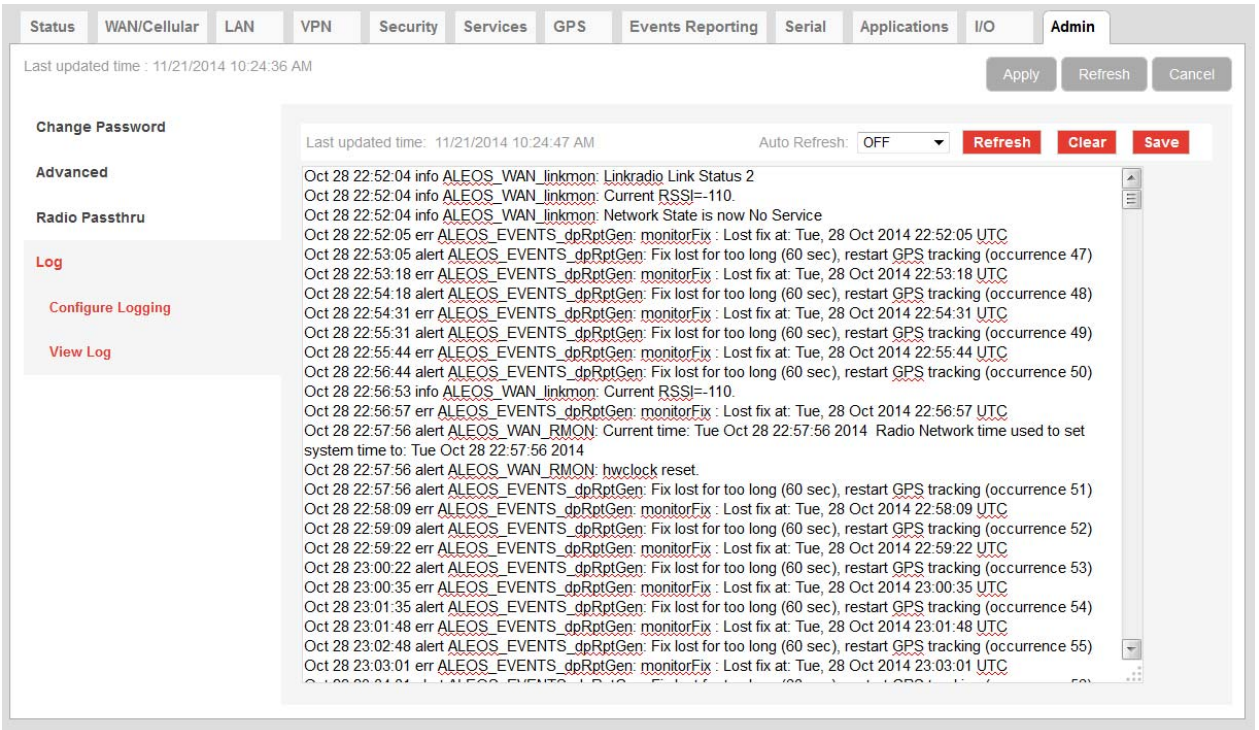

Status
WAN/Cellular
LAN
VPN
Security
Services
GPS
Events Reporting
Serial
Applications
I/O
Admin
Last updated time : 11/21/2014 10:24:36 AM
Apply
Refresh
Cancel
Change Password
Advanced
Radio Passthru
Log
Configure Logging
View Log
Last updated time: 11/21/2014 10:24:47 AM
Auto Refresh: OFF
Refresh
Clear
Save
Oct 28 22:52:04 info ALEOS_WAN_linkmon: Linkradio Link Status 2
Oct 28 22:52:04 info ALEOS_WAN_linkmon: Current RSSI=-110.
Oct 28 22:52:04 info ALEOS_WAN_linkmon: Network State is now No Service
Oct 28 22:52:05 err ALEOS_EVENTS_dpRptGen: monitorFix : Lost fix at: Tue, 28 Oct 2014 22:52:05 UTC
Oct 28 22:53:05 alert ALEOS_EVENTS_dpRptGen: Fix lost for too long (60 sec), restart GPS tracking (occurrence 47)
Oct 28 22:53:18 err ALEOS_EVENTS_dpRptGen: monitorFix : Lost fix at: Tue, 28 Oct 2014 22:53:18 UTC
Oct 28 22:54:18 alert ALEOS_EVENTS_dpRptGen: Fix lost for too long (60 sec), restart GPS tracking (occurrence 48)
Oct 28 22:54:31 err ALEOS_EVENTS_dpRptGen: monitorFix : Lost fix at: Tue, 28 Oct 2014 22:54:31 UTC
Oct 28 22:55:31 alert ALEOS_EVENTS_dpRptGen: Fix lost for too long (60 sec), restart GPS tracking (occurrence 49)
Oct 28 22:55:44 err ALEOS_EVENTS_dpRptGen: monitorFix : Lost fix at: Tue, 28 Oct 2014 22:55:44 UTC
Oct 28 22:56:44 alert ALEOS_EVENTS_dpRptGen: Fix lost for too long (60 sec), restart GPS tracking (occurrence 50)
Oct 28 22:56:53 info ALEOS_WAN_linkmon: Current RSSI=-110.
Oct 28 22:56:57 err ALEOS_EVENTS_dpRptGen: monitorFix : Lost fix at: Tue, 28 Oct 2014 22:56:57 UTC
Oct 28 22:57:56 alert ALEOS_WAN_RMON: Current time: Tue Oct 28 22:57:56 2014 Radio Network time used to set system time to: Tue Oct 28 22:57:56 2014
Oct 28 22:57:56 alert ALEOS_WAN_RMON: hwclock reset.
Oct 28 22:57:56 alert ALEOS_EVENTS_dpRptGen: Fix lost for too long (60 sec), restart GPS tracking (occurrence 51)
Oct 28 22:58:09 err ALEOS_EVENTS_dpRptGen: monitorFix : Lost fix at: Tue, 28 Oct 2014 22:58:09 UTC
Oct 28 22:59:09 alert ALEOS_EVENTS_dpRptGen: Fix lost for too long (60 sec), restart GPS tracking (occurrence 52)
Oct 28 22:59:22 err ALEOS_EVENTS_dpRptGen: monitorFix : Lost fix at: Tue, 28 Oct 2014 22:59:22 UTC
Oct 28 23:00:22 alert ALEOS_EVENTS_dpRptGen: Fix lost for too long (60 sec), restart GPS tracking (occurrence 53)
Oct 28 23:00:35 err ALEOS_EVENTS_dpRptGen: monitorFix : Lost fix at: Tue, 28 Oct 2014 23:00:35 UTC
Oct 28 23:01:35 alert ALEOS_EVENTS_dpRptGen: Fix lost for too long (60 sec), restart GPS tracking (occurrence 54)
Oct 28 23:01:48 err ALEOS_EVENTS_dpRptGen: monitorFix : Lost fix at: Tue, 28 Oct 2014 23:01:48 UTC
Oct 28 23:02:48 alert ALEOS_EVENTS_dpRptGen: Fix lost for too long (60 sec), restart GPS tracking (occurrence 55)
Oct 28 23:03:01 err ALEOS_EVENTS_dpRptGen: monitorFix : Lost fix at: Tue, 28 Oct 2014 23:03:01 UTC

Figure 14-5: ACEmanager: Admin > Log, View Log

Note: VPN info and debug information uses the term racoon (rather than VPN), as shown in Figure 14-5.

Note: If you toggle the "Display in Log?" field, clear and refresh the View Log page. (You do not need to reboot the device.)

Tip: *Use View Log for troubleshooting purposes (e.g., when setting up the IPsec configuration). The Log page allows you to establish the tunnel connection and monitor the results directly. To change the intervals at which the log is displayed, you can change the settings in Auto Refresh.*

Actions on the View Log screen include:

- Auto Refresh — The drop-down menu allows you to set up an automatic log page refresh, and the interval between refreshes: 30 secs, 1 minute, or 2 minutes.
- Refresh button — Initiates a manual page refresh
- Clear button — Clears out the tunnels
- Save button — Creates a text file of the log

A: Windows Dial-up Networking (DUN)

Dial-up Networking (DUN) enables you to use Point-to-Point Protocol (PPP) to establish a connection between a host PC serial port and the AirLink device, as shown in Figure A-1.

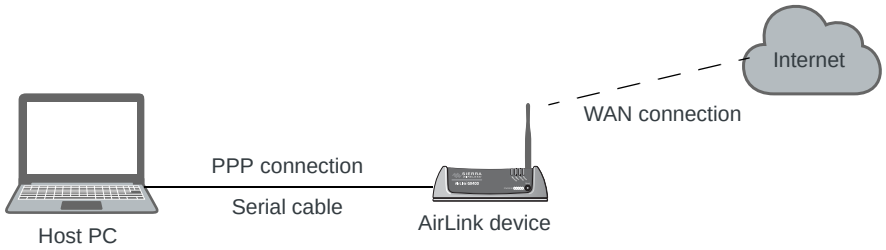


Figure A-1: PPP connection

Caution: *To install any driver on your computer, you may need to be logged in as Administrator or have Administrator privileges for your login.*

Microsoft Windows 7 is used in the examples below. The device driver installation and DUN setup and configuration is similar in other Microsoft Windows operating systems, including Windows XP and Windows CE.

Note: If your device is new, or has recently been reset to factory default settings, ensure that the device has been on air at least once before being used with a DUN connection.

Installing a Device Driver

Connect the AirLink device

1. Connect the device to the computer with a DB-9 cable from one RS-232 port to the other.
2. Log in to ACEmanager.
3. Go to Serial > Port Configuration.
4. Set the DB9 Serial Echo field to Disable.
5. Reboot.

Note: You need to set the DB9 Serial Echo field echo to Disable any time you want to set up a PPP connection.

Install the driver

1. Select Start > Control Panel > Phone and Modem Options.

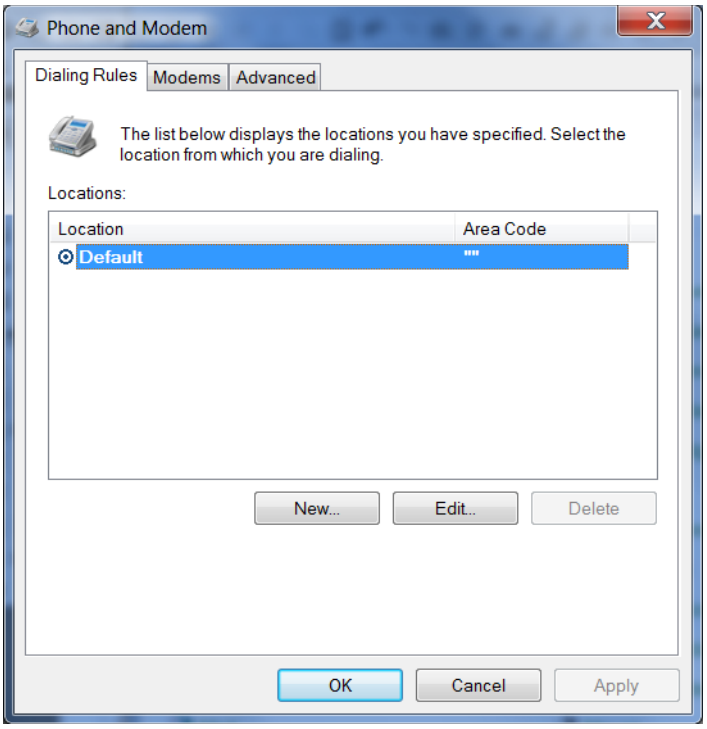


Figure A-2: Phone and Modem Options

2. Select the Modems tab.

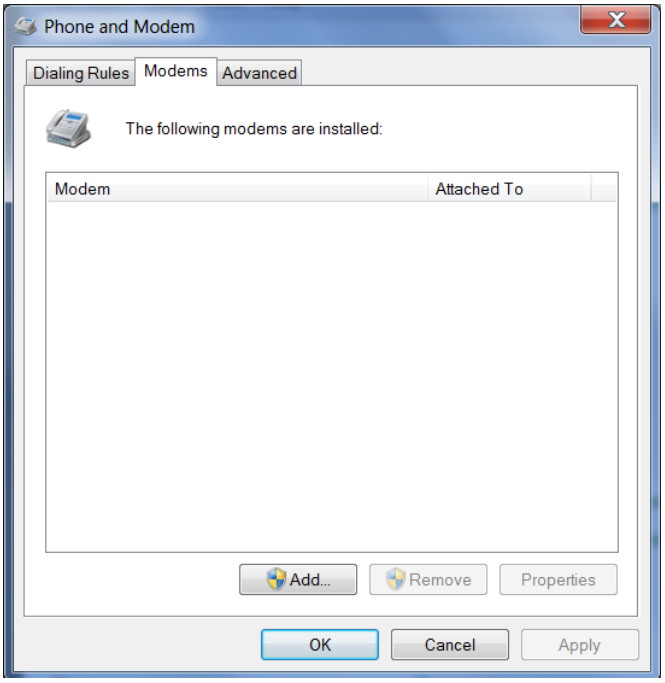


Figure A-3: Phone and Modem Options: devices

3. Click Add.

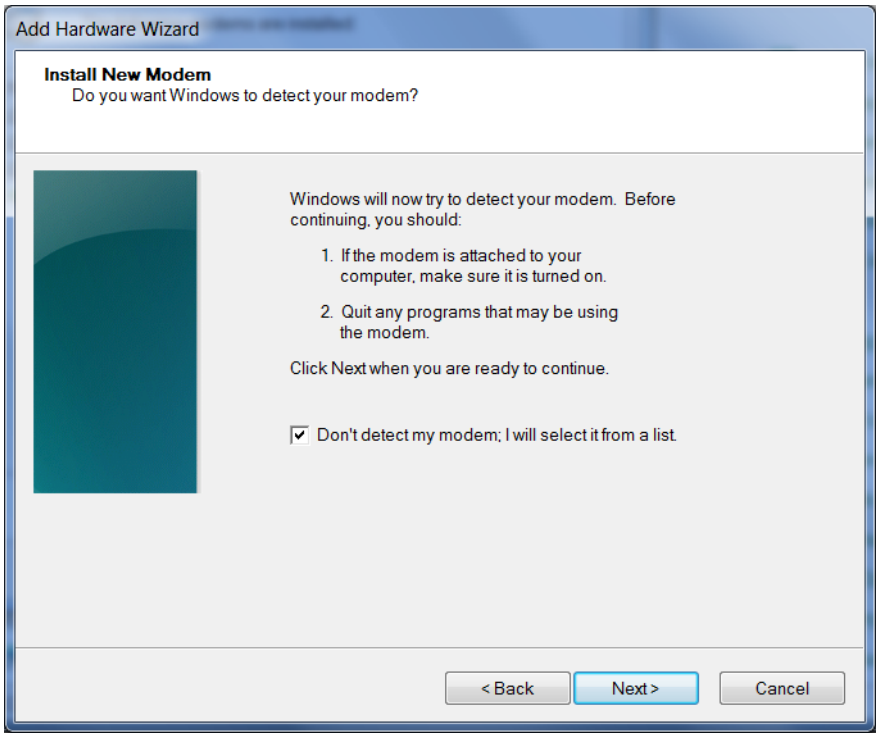

Add Hardware Wizard
Install New Modem
Do you want Windows to detect your modem?
Windows will now try to detect your modem. Before continuing, you should:
1. If the modem is attached to your computer, make sure it is turned on.
2. Quit any programs that may be using the modem.
Click Next when you are ready to continue.
Don't detect my modem; I will select it from a list.
< Back
Next >
Cancel

Figure A-4: Add Hardware Wizard

4. Select Don’t detect my modem; I will select it from a list.
5. Click Next.

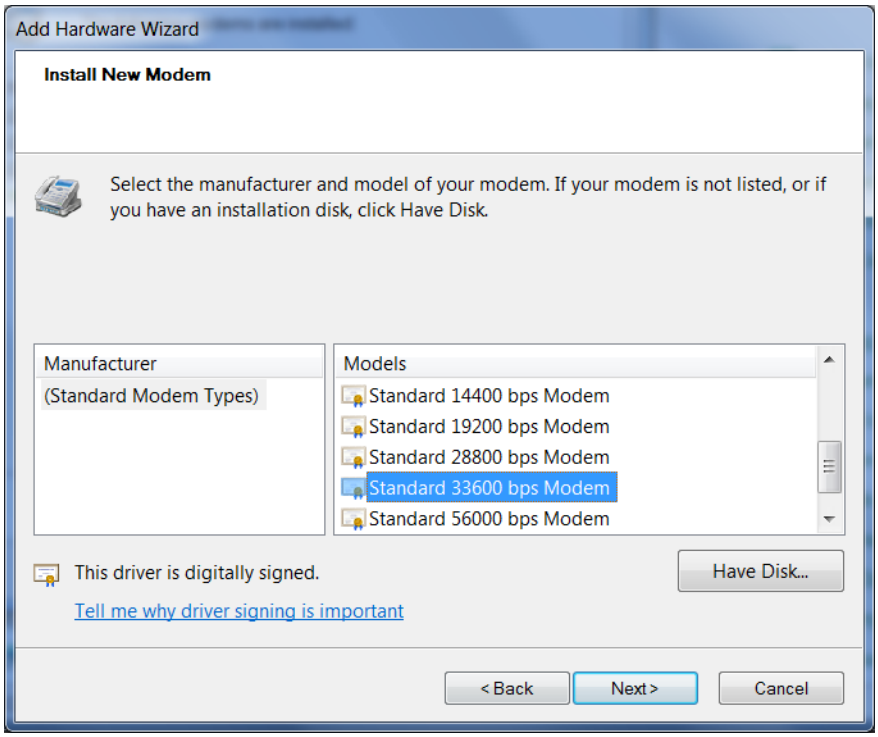

Add Hardware Wizard
Install New Modem
Select the manufacturer and model of your modem. If your modem is not listed, or if you have an installation disk, click Have Disk.
Manufacturer
(Standard Modem Types)
Models
Standard 14400 bps Modem
Standard 19200 bps Modem
Standard 28800 bps Modem
Standard 33600 bps Modem
Standard 56000 bps Modem
This driver is digitally signed.
Have Disk...
Tell me why driver signing is important
< Back
Next >
Cancel

Figure A-5: Add Hardware Wizard: Install New Modem

6. Under Manufacturer, select (Standard Modem Types).
7. Under Models, select Standard 33600 bps Modem.

Tip: *If you have the speed for your device configured as something other than the default, use the Standard device that matches the speed you configured.*

8. Click Next.

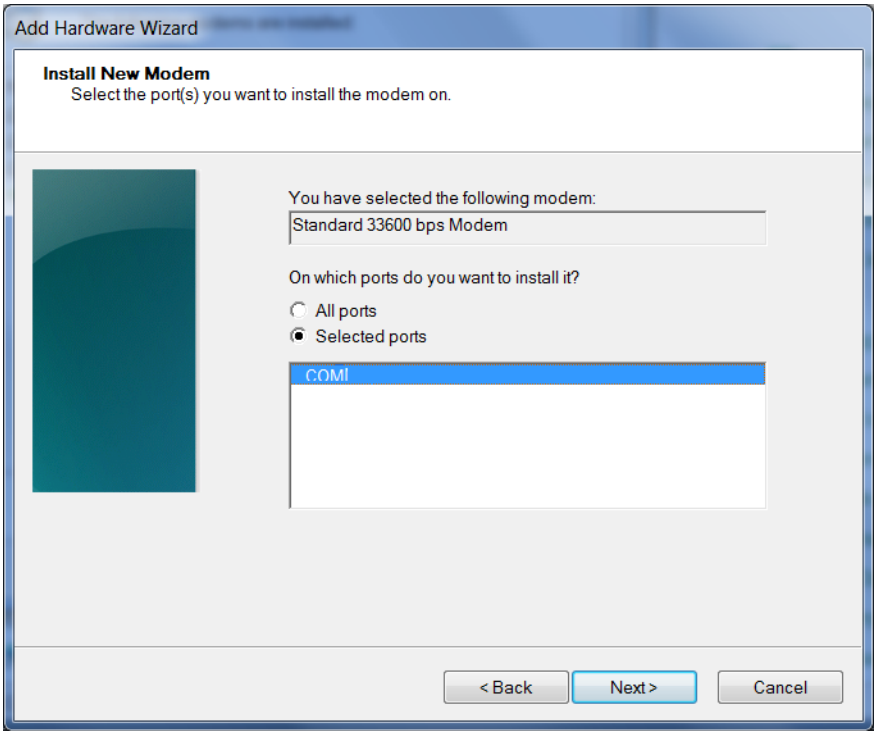

Add Hardware Wizard
Install New Modem
Select the port(s) you want to install the modem on.
You have selected the following modem:
Standard 33600 bps Modem
On which ports do you want to install it?
All ports
Selected ports
COM1
< Back
Next >
Cancel

Figure A-6: Add Hardware Wizard: Select Ports

9. Select Selected Ports.
10. Select the COM port the device is connected to (commonly COM1).
11. Click Next.

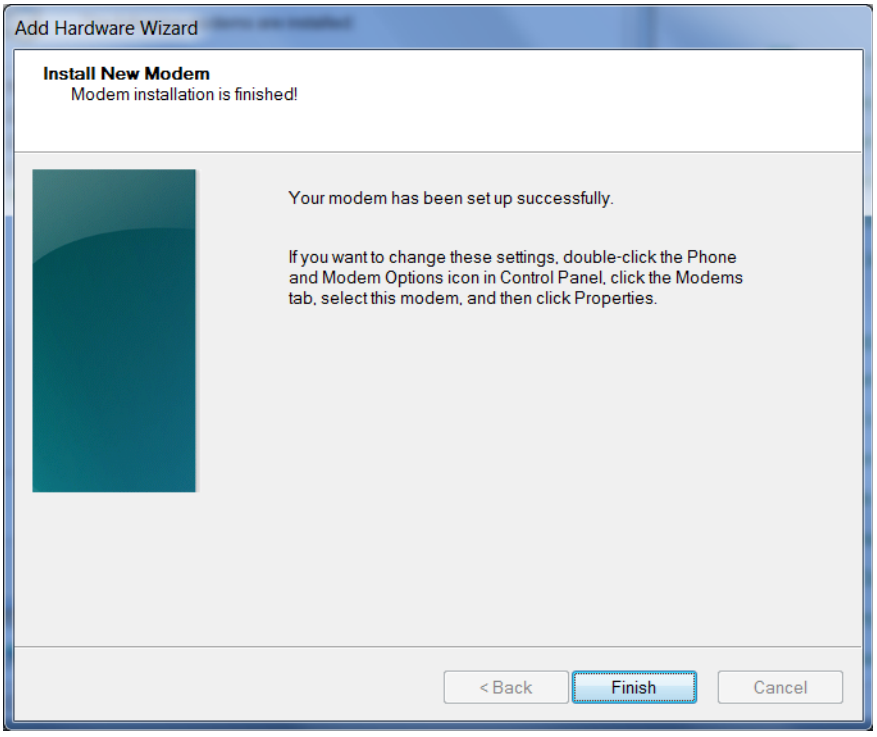

Add Hardware Wizard
Install New Modem
Modem installation is finished!
Your modem has been set up successfully.
If you want to change these settings, double-click the Phone and Modem Options icon in Control Panel, click the Modems tab, select this modem, and then click Properties.
< Back
Finish
Cancel

Figure A-7: Add Hardware Wizard: Finish

12. Once the device driver is installed, click Finish.

When you return to the Phone and Modem Options page, you should see the newly installed device “attached to” the correct COM port.

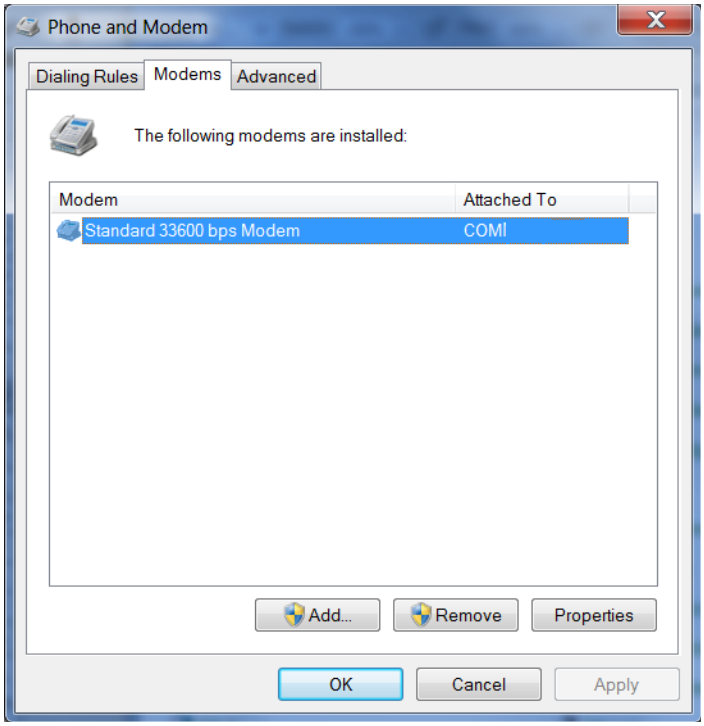


Figure A-8: Phone and Modem Options > Modems

13. Highlight the modem, and click Properties. The following window appears:

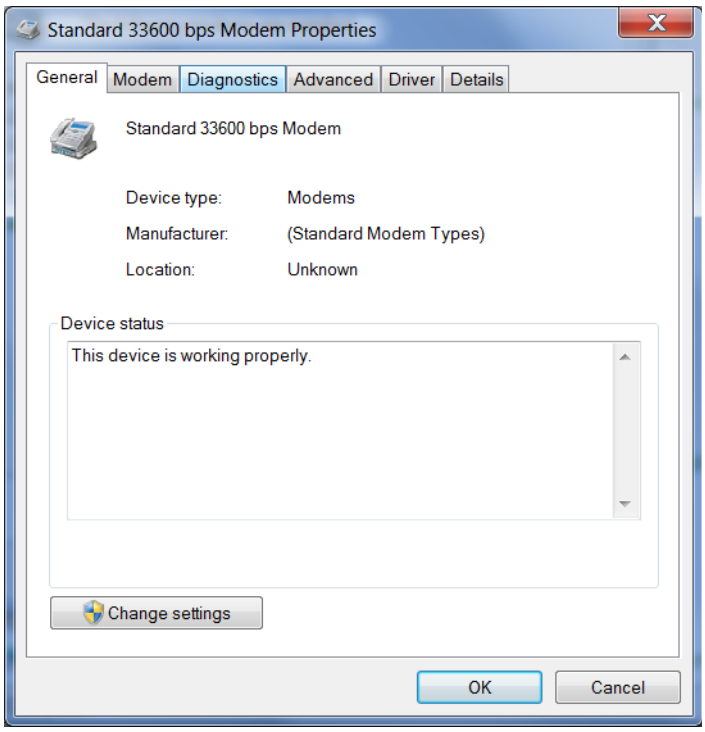


Figure A-9: Modem Properties

14. Select the Modem tab.

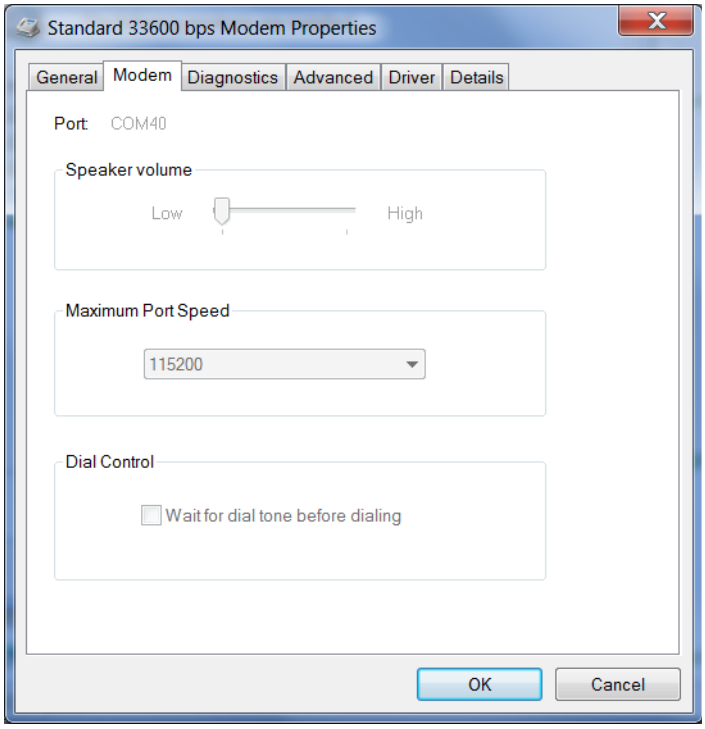


Figure A-10: Modem Properties > Modem

15. Confirm that the Maximum Port Speed is set to 115200 (default).

16. Click OK to exit.
17. Click OK again to exit out of the Phone and Modem Options.
18. Go to Start > Control Panel > Device Manager.

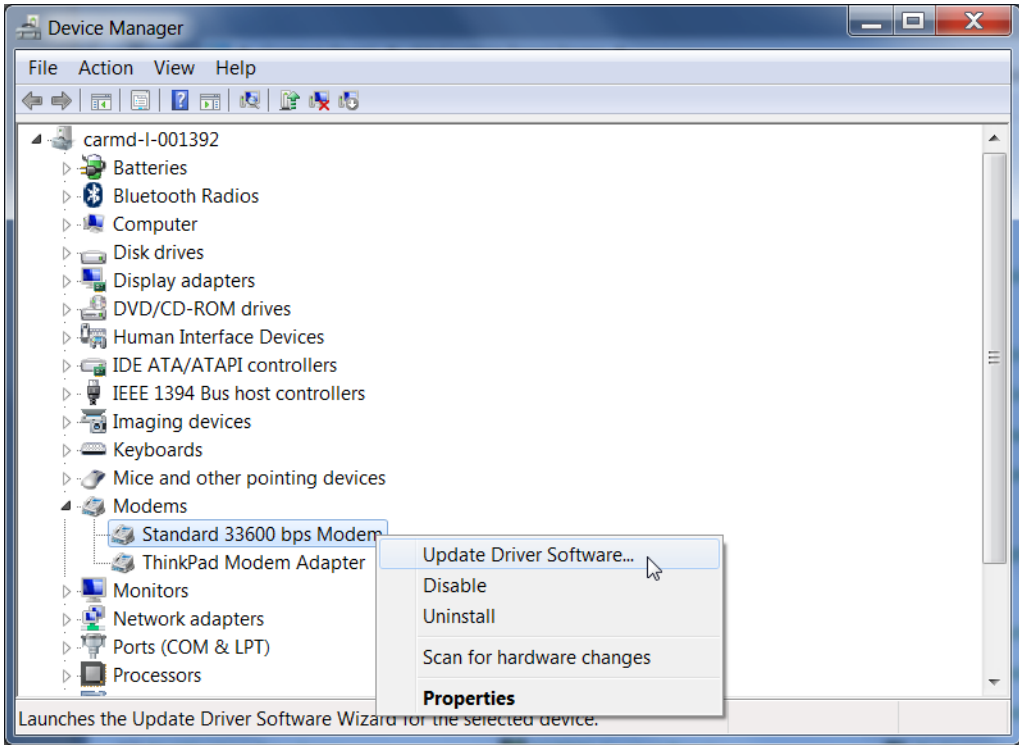


Figure A-11: Device Manager

19. Under Modems, highlight Standard 33600 bps Modem. Right-click and select Update Driver Software....

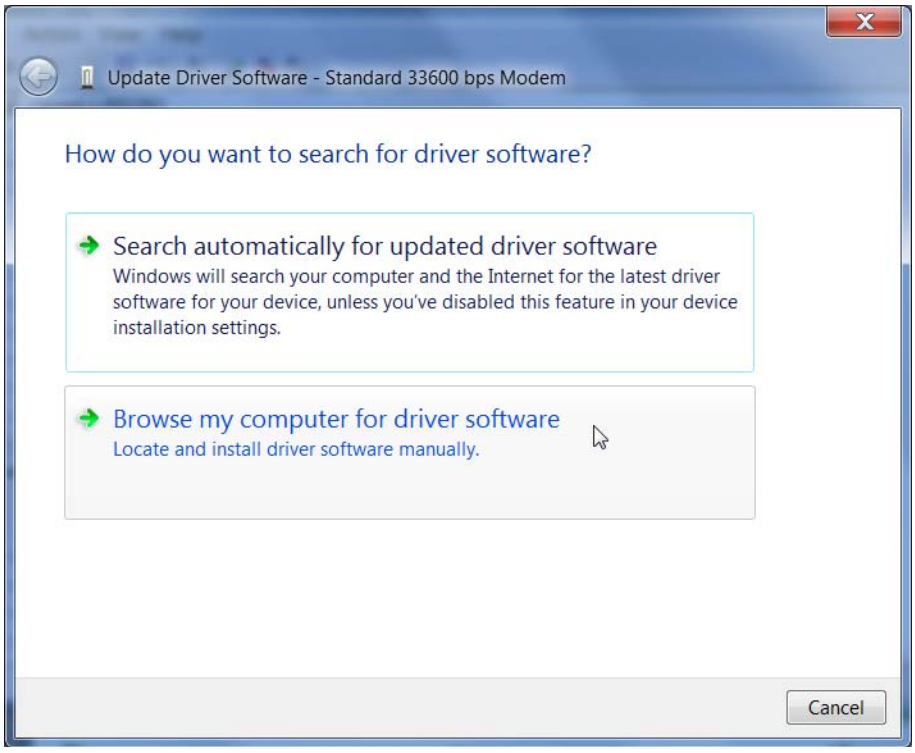

Update Driver Software - Standard 33600 bps Modem
How do you want to search for driver software?
Search automatically for updated driver software
Windows will search your computer and the Internet for the latest driver software for your device, unless you've disabled this feature in your device installation settings.
Browse my computer for driver software
Locate and install driver software manually.
Cancel

Figure A-12: Update Driver Software—Browse

20. Select Browse my computer for driver software.

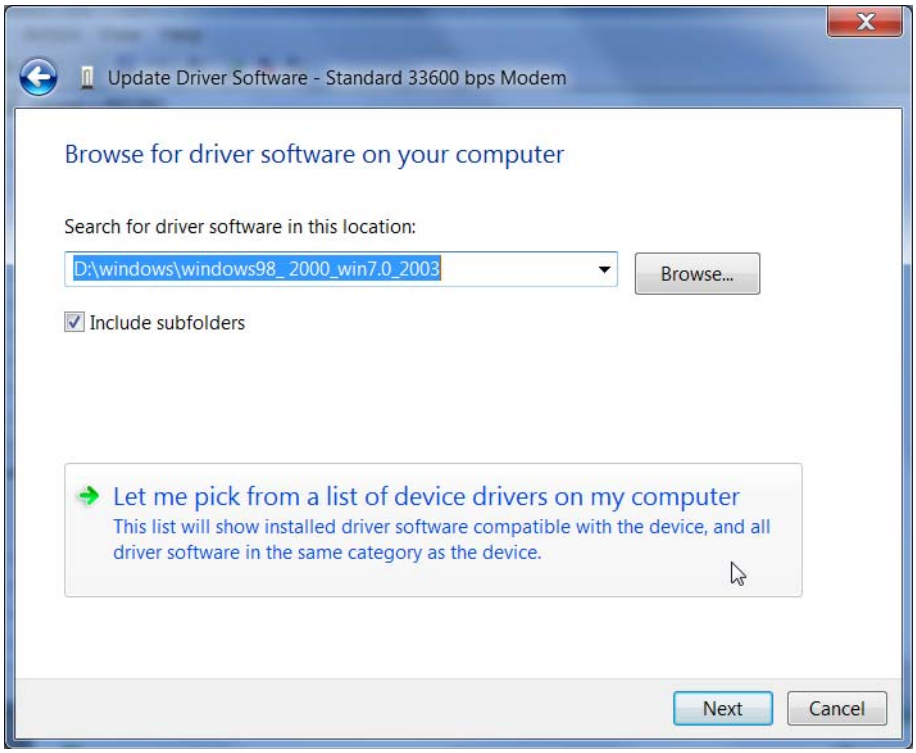

Update Driver Software - Standard 33600 bps Modem
Browse for driver software on your computer
Search for driver software in this location:
D:\windows\windows98_2000_win7.0_2003
Browse...
Include subfolders
Let me pick from a list of device drivers on my computer
This list will show installed driver software compatible with the device, and all driver software in the same category as the device.
Next
Cancel

Figure A-13: Update Driver Software—Let me pick...

21. Select Let me pick from a list of device drivers on my computer.

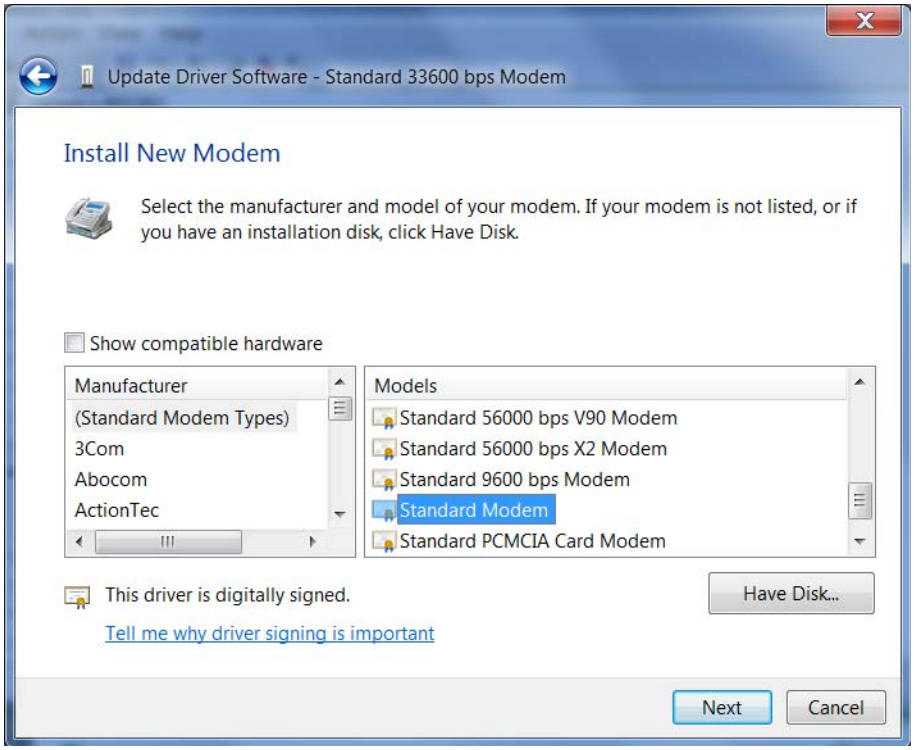

Update Driver Software - Standard 33600 bps Modem
Install New Modem
Select the manufacturer and model of your modem. If your modem is not listed, or if you have an installation disk, click Have Disk.
Show compatible hardware
Manufacturer
(Standard Modem Types)
3Com
Abocom
ActionTec
Models
Standard 56000 bps V90 Modem
Standard 56000 bps X2 Modem
Standard 9600 bps Modem
Standard Modem
Standard PCMCIA Card Modem
This driver is digitally signed.
Have Disk...
Tell me why driver signing is important
Next
Cancel

Figure A-14: Update Driver Software—Select Standard Modem

22. Deselect Show compatible hardware.
23. Under Manufacturer, select (Standard Modem Types).
24. Under Models, select Standard Modem.
25. Click Next.

    If you see an Update Driver Warning, click Yes.

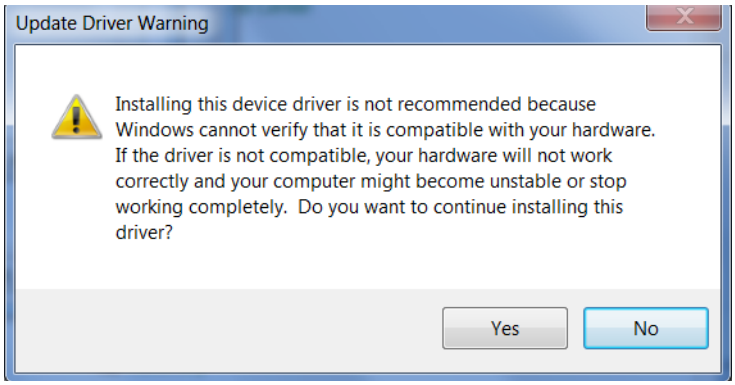

Update Driver Warning
Installing this device driver is not recommended because Windows cannot verify that it is compatible with your hardware. If the driver is not compatible, your hardware will not work correctly and your computer might become unstable or stop working completely. Do you want to continue installing this driver?
Yes
No

Figure A-15: Update Driver Software—Warning

The software driver updates and the following window appears:

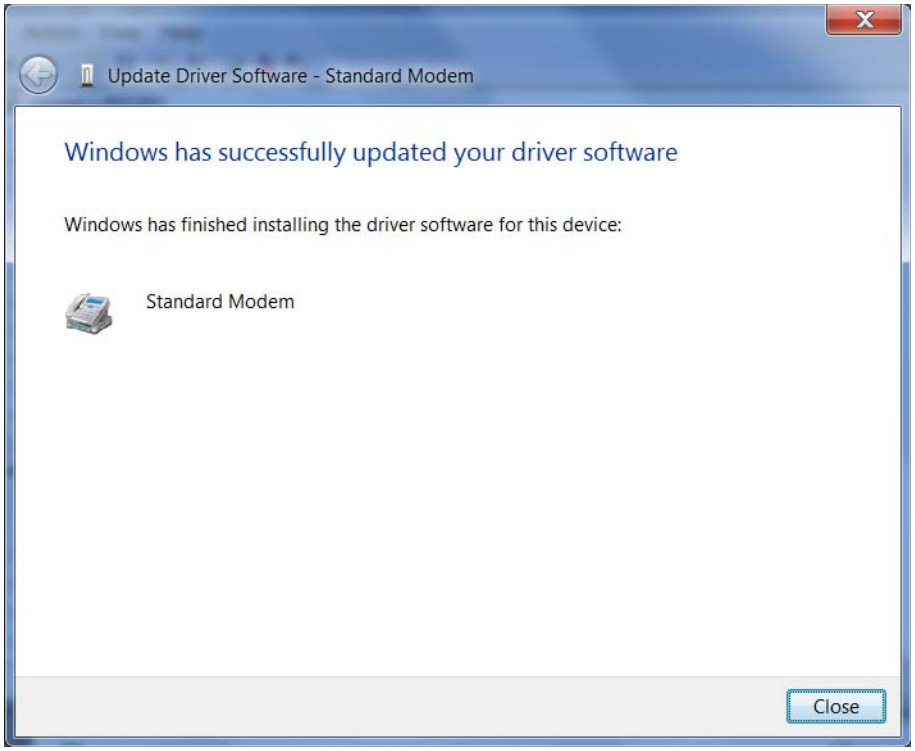

Update Driver Software - Standard Modem
Windows has successfully updated your driver software
Windows has finished installing the driver software for this device:
Standard Modem
Close

Figure A-16: Update Driver Software—Success

26. Click Close.

Creating a Dial-Up Networking (PPP) Connection

Once you have the driver for the modem installed on your computer, you can set up and configure Dial Up Networking (DUN).

Note: No other device or program can use the COM port (serial port) configured for the modem driver while the DUN session is active.

Caution: *If you have an existing LAN connection, installing DUN for the AirLink device may interfere with the LAN connection. We recommend disconnecting your LAN connection before using a PPP connection with your AirLink device.*

Once you have configured the DUN connection on your computer:

- The DUN connection may be set as the default connection.
- The computer may be configured to dial the DUN connection when it cannot detect any network connection.

For instructions on changing these options, see Connection settings on page 351.

If you are using a DUN connection with any other network connection (such as Ethernet or Wi-Fi), you may need to use the route command in Windows to set up a static route through the device to access the location remotely over the PPP link and the cellular network. This guide does not provide information on the route command. Consult your network administrator for information on properly configuring routing.

Create a new network connection.

1. Select Start > Control Panel > Network and Sharing Center.

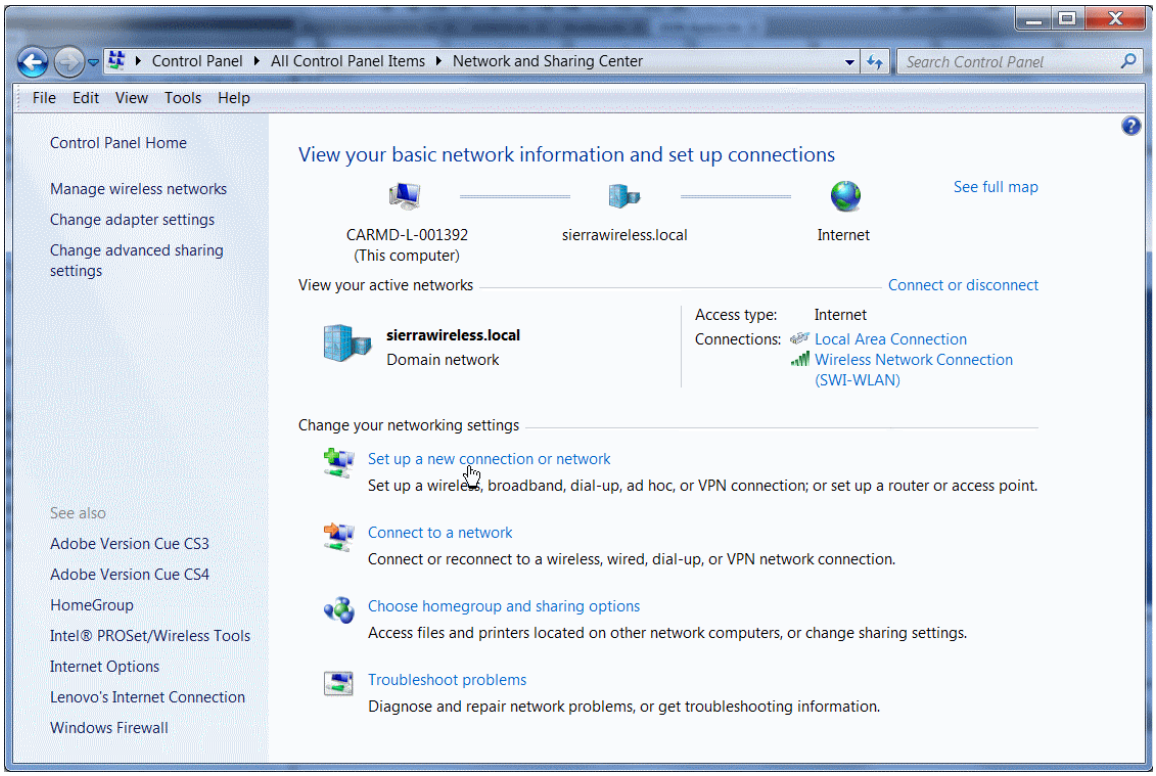

Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center
Search Control Panel
File Edit View Tools Help
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
CARMD-L-001392 (This computer)
sierrawireless.local
Internet
View your active networks
Connect or disconnect
sierrawireless.local
Domain network
Access type: Internet
Connections: Local Area Connection
Wireless Network Connection (SWI-WLAN)
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.
Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
Adobe Version Cue CS3
Adobe Version Cue CS4
HomeGroup
Intel® PROSet/Wireless Tools
Internet Options
Lenovo's Internet Connection
Windows Firewall

Figure A-17: Network and Sharing Center Window

2. Select Set up a new connection or network.

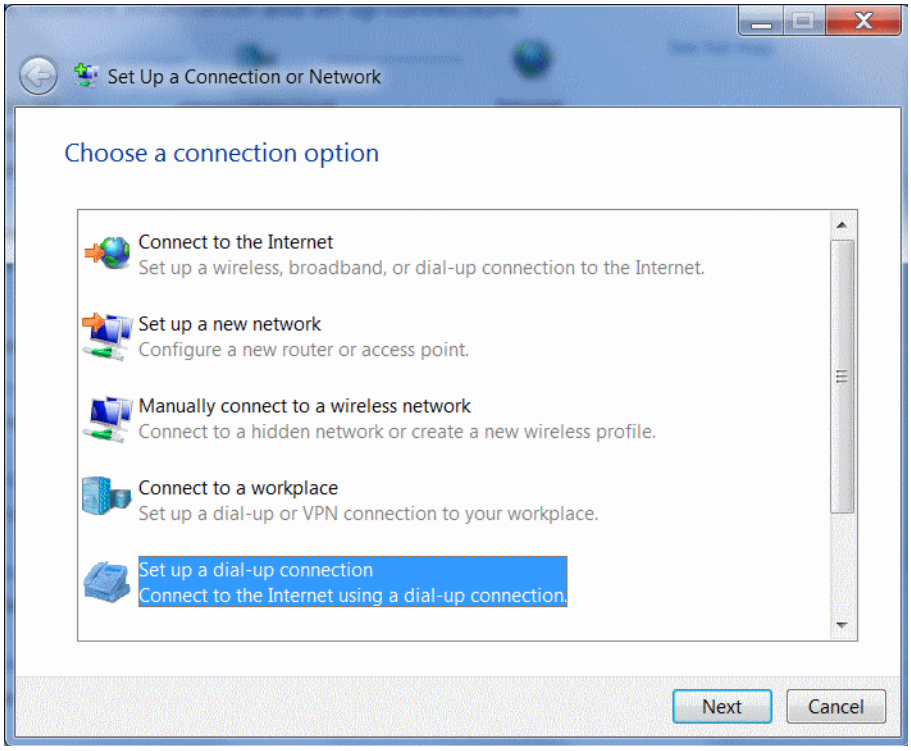

Set Up a Connection or Network
Choose a connection option
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.
Set up a new network
Configure a new router or access point.
Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.
Set up a dial-up connection
Connect to the Internet using a dial-up connection.
Next
Cancel

Figure A-18: Set up a Connection or Network

3. Select Set up a dial-up connection.
4. Click Next.

   If you are asked which modem you want to use, select Standard Modem.

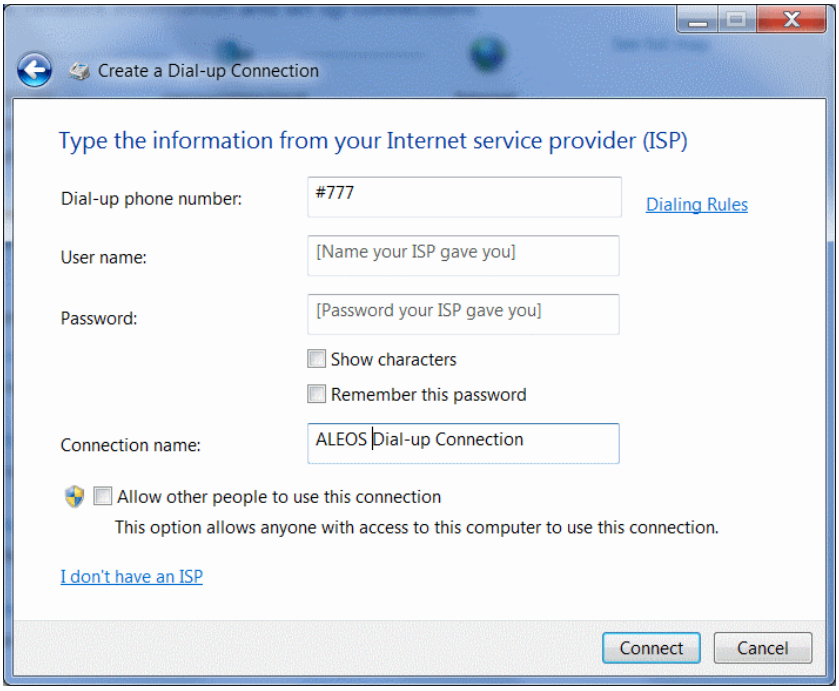


Figure A-19: Create a Dial up Connection

5. In the Dial-up phone number field, type “#777”.
6. Ignore the User name and Password fields.
7. In the Connection name field, type “ALEOS Dial-up Connection” or other desired name.
8. Click Connect.

   Alternatively, to connect to the ALEOS Dial-up network:

   a. Click the network connection icon[1] in the system tray.
   b. Select ALEOS Dial-up Connection.
   c. Click Connect.

Configure the DUN connection

After you complete the New Connection Wizard:

1. Click the network connection icon, select ALEOS Dial-up Connection, and click Connect.

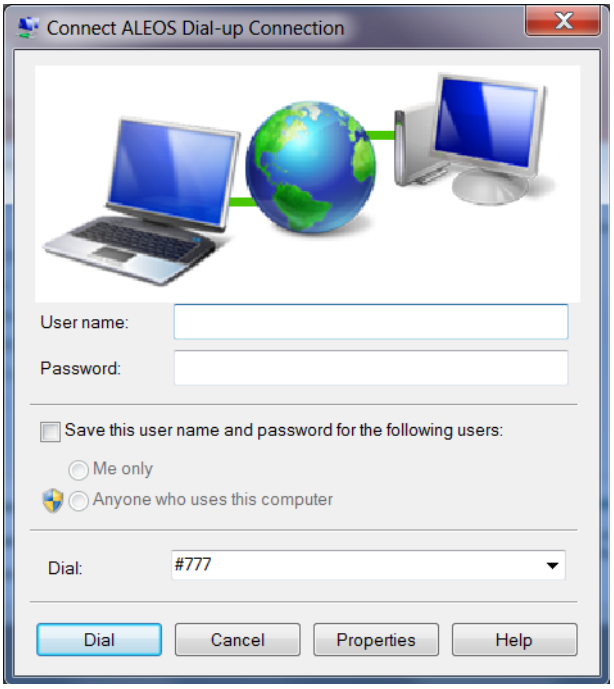


Figure A-20: DUN Connection

2. If you have a user name and password configured in ACEmanager for PPP connections, enter them in the User name and Password fields. Otherwise, leave these fields blank.
3. Click Properties.

1. The appearance of the connection icon varies depending on the type of connections available. For example, It may appear as , , or .

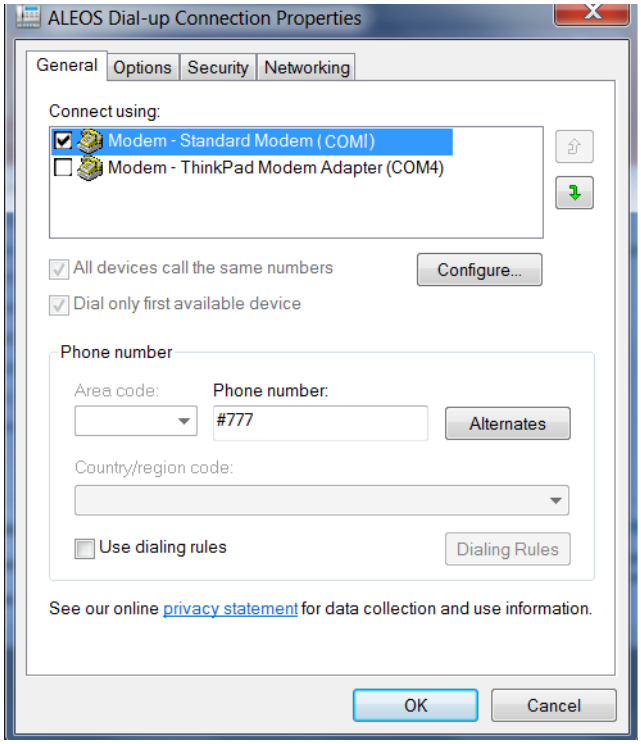


Figure A-21: DUN Properties

4. Confirm that the check box beside Use dialing rules is not selected.
5. Click Configure... (below the Connect using box).

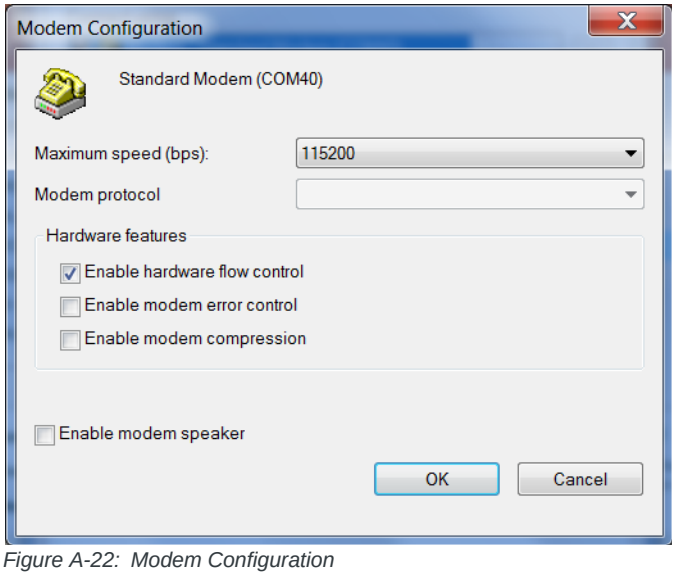


Figure A-22: Modem Configuration

6. Confirm that the Maximum speed (bps) is set to 115200.
7. Confirm that Enable hardware flow control is selected. Do not select any other options.
8. Click OK.

9. In the main properties window, select the Options tab.

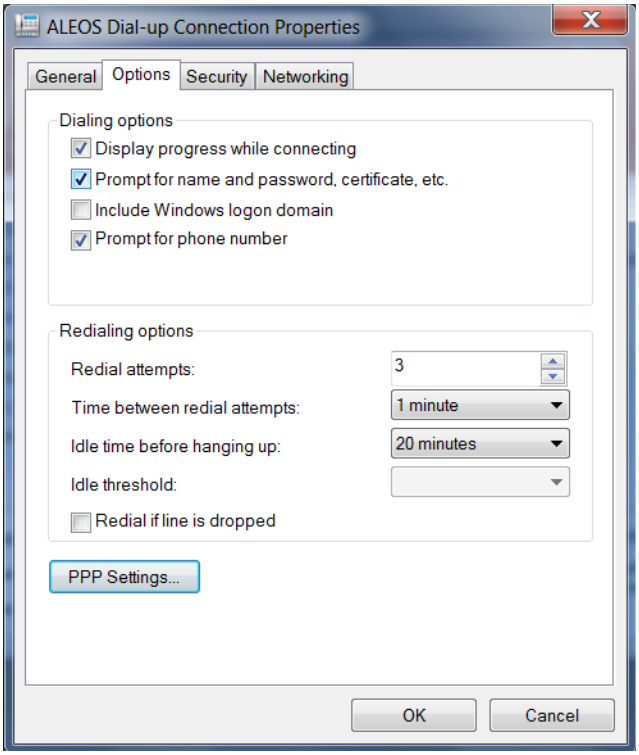


Figure A-23: Networking

10. Click PPP Settings.

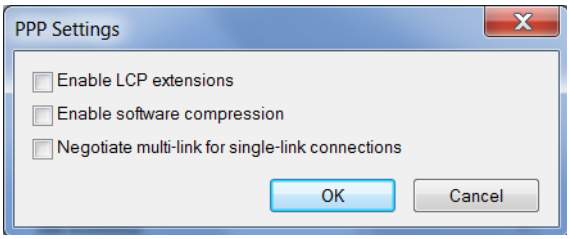


Figure A-24: PPP Settings

11. Clear the check boxes beside all three PPP settings.
12. Click OK.
13. Select the Networking tab.

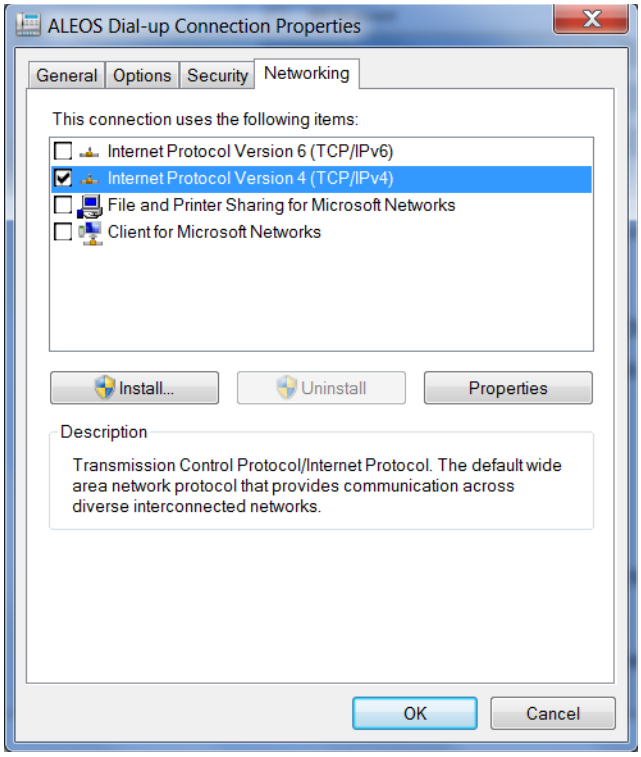


Figure A-25: DUN Connection > Networking tab

14. Select Internet Protocol Version 4 (TCP/IPv4) and then select Properties.

Tip: *For most configurations, getting the IP address and the DNS server address are automatic.*

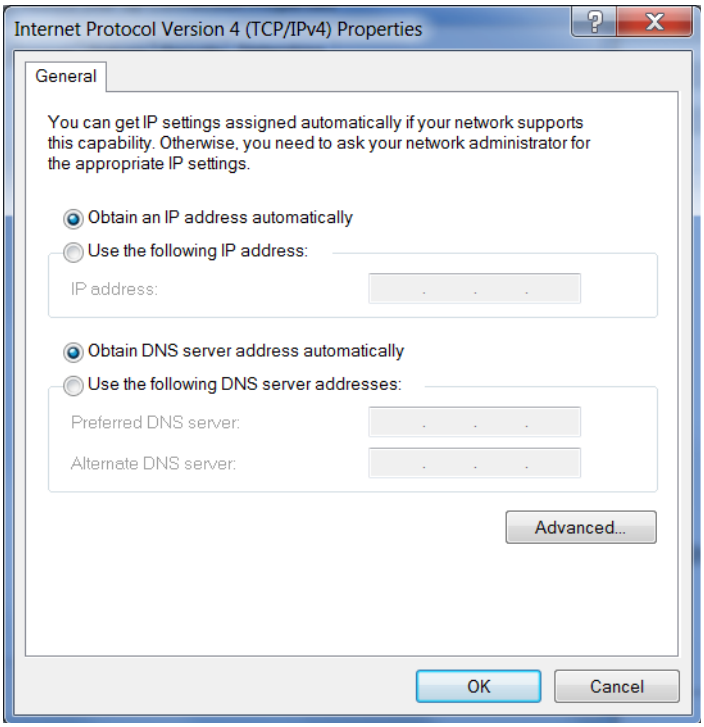

Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Figure A-26: TCP/IP Properties

15. Click Advanced.

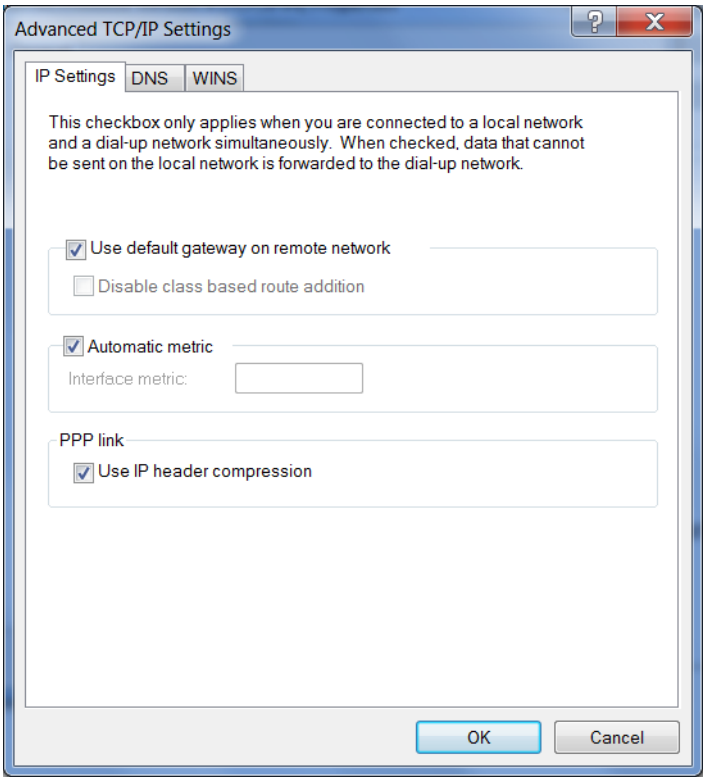

Advanced TCP/IP Settings
IP Settings
DNS
WINS
This checkbox only applies when you are connected to a local network and a dial-up network simultaneously. When checked, data that cannot be sent on the local network is forwarded to the dial-up network.
Use default gateway on remote network
Disable class based route addition
Automatic metric
Interface metric:
PPP link
Use IP header compression
OK
Cancel

Figure A-27: Advanced TCP/IP

16. Select Use default gateway on remote network.
17. Click OK.

Tip: *You may want to check the Options tab and change the settings for applications you use. The default options are generally applicable for most uses.*

Caution: *Unless specifically directed to do so by Support or your network administrator, you do not need to make any changes to the options on the Security tab.*

18. Click OK until you return to the Connect window.
19. Log in to ACEmanager and go to Serial > Port Configuration.

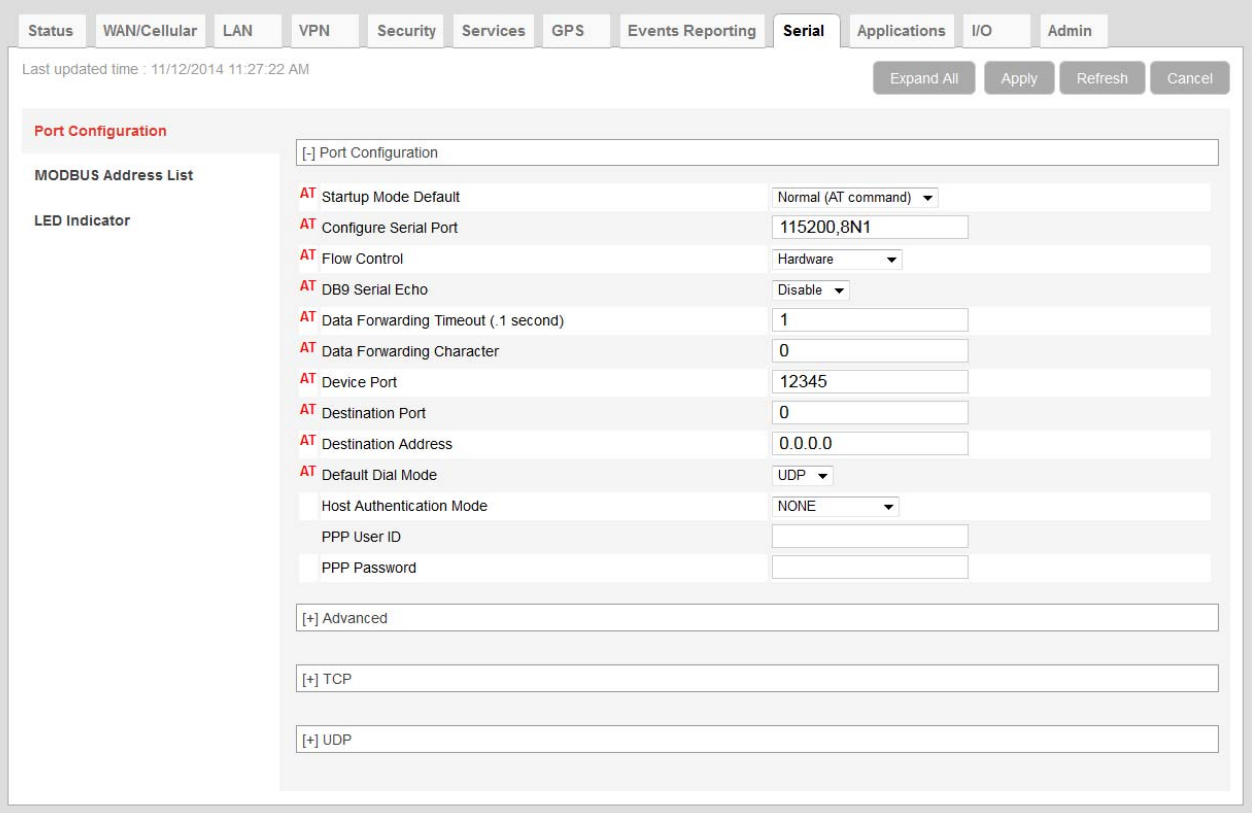


Figure A-28: ACEmanager: Serial > Port Configuration

20. Under Port Configuration:
    a. Set the Flow Control field to Hardware.
    b. Set the DB9 Serial Echo field to Disable.
21. Click Apply and reboot the device.

Connection settings

1. To set the default connection:
2. Go to Start > Control Panel > Network and Sharing Center.

3. Select Change adapter settings.
4. Right-click the icon for the DUN connection.

   If you want this to be your default connection, select Set as Default Connection.

   If it is already the default connection and you do not want it as your default connection, select Cancel as Default Connection.

If you do not want the DUN connection to be dialed when there is no other connection:

1. Go to Start > Control Panel > Internet Options.
2. Select the Connections tab.
3. Highlight the DUN connection and select Never dial a connection.
4. Click Apply.
5. Click OK.

Connecting to the Internet Using DUN

There are two methods you can use to connect the AirLink device to a host PC using DUN: ACEview, and the Windows DUN direct connection.

ACEview

ACEview is a utility which can maintain your DUN connection and monitor the connection of your AirLink device to the provider. If you have not already installed ACEview, obtain the most recent version from the Sierra Wireless AirLink website.

This guide assumes you have a default installation of ACEview.

1. Start ACEview.

   Go to Start > All Programs > Sierra Wireless > ACEview
2. Right-click the ACEview window to open the menu.

Figure A-29: ACEview: Menu

3. Select Settings.

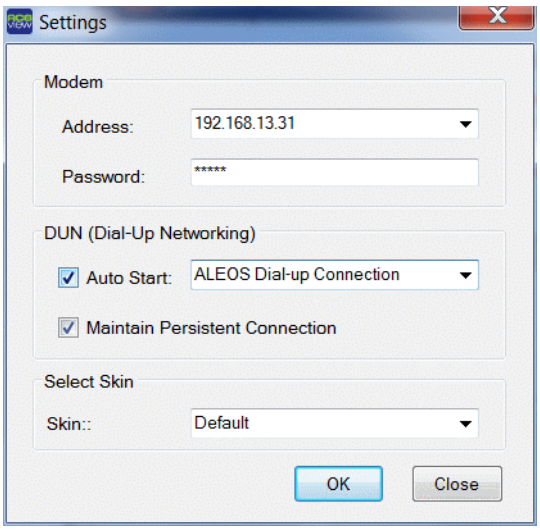


Figure A-30: ACEview: Connection Settings

4. Select Auto Start in the DUN section.
5. Select Maintain Persistent Connection.

   When selected, ACEview continually checks the DUN connection to ensure it is not down. If the connection is down, ACEview attempts to reconnect.

Tip: *When using the DUN connection, make sure the IP Address is set to the local IP address of the modem, i.e., 192.168.13.31 (by default).*

6. Click OK.

Windows DUN

You can directly use the Dial-up link for the DUN connection.

To start the DUN session:

1. Click the network connection icon (), select ALEOS Dial-up Connection, and click Connect.

   When you are connected, an icon should appear in the system tray showing the connection status.

Note: The speed shown in the connection is the speed between the modem and your computer. It is not the speed of the modem's connection to the provider or the Internet.

Caution: *For DUN connections on a Windows Mobility or other non-personal computer, the DNS settings may not be configured with the DUN connection. Go into the network settings and add DNS servers manually.*

B: Modbus/BSAP Configuration

B

The AirLink device supports Modbus ASCII, Modbus RTU, and BSAP, and can also emulate other protocols (like DF1) using the Modbus Variable feature.

Modbus Overview

The Modbus Protocol provides for client-server (i.e., master-slave) communications between intelligent devices. As a de facto standard, it is the most widely used network protocol in the industrial manufacturing environment to transfer discrete/analog I/O and register data between control devices. Modbus, BSAP, and other Modbus variations are often used in conjunction with telemetry devices.

Tip: *This section is just a brief overview of Modbus. For more information, refer to your Modbus equipment distributor or manufacturer or www.modbus.org.*

Telemetry

Telemetry is an automated communications process by which data is collected from instruments located at remote or inaccessible points and transmitted to receiving equipment for measurement, monitoring, display, and recording. Transmission of the information may be over physical pairs of wires, telecommunication circuits, radios, or satellites.

Remote Terminal Unit (RTU)

Modbus was originally designed to be used in a radio environment where packets were broadcast from a central station (i.e., master or host) to a group of remote units. Each remote unit, or Remote Terminal Unit (RTU), has a hexadecimal identification number (ID). The first part of the broadcast packet contains an RTU ID which corresponds to the ID of one of the remote units. The Modbus host looks for the ID and only sends to the unit with the matching ID; the RTU then replies back to the central station.

The RTU connects to such physical equipment as switches, pumps, and other devices, and monitors and controls these devices. The RTU can be part of a network set up for Supervisory Control and Data Acquisition.

Supervisory Control and Data Acquisition (SCADA)

Supervisory Control and Data Acquisition (SCADA) describes solutions across a large variety of industries and is used in industrial and engineering applications to monitor and control distributed systems from a master location. SCADA encompasses multiple RTUs, a central control room with a host computer (or network), and some sort of communication infrastructure.

SCADA allows for “supervisory” control of remote devices as well as acquiring data from the remote locations. Programmable Logic Controllers allow for a higher degree of automated SCADA.

Programmable Logic Controller (PLC)

A Programmable Logic Controller (PLC) is a small industrial computer which generally monitors several connected sensor inputs and controls attached devices (motor starters, solenoids, pilot lights/displays, speed drives, valves, etc.) according to a user-created program stored in its memory. Containing inputs and outputs similar to an RTU, PLCs are frequently used for typical relay control, sophisticated motion control, process control, Distributed Control System and complex networking.

Modbus TCP/IP

Modbus TCP/IP simply takes the Modbus instruction set and wraps TCP/IP around it. Since TCP/IP is the communications standard for the Internet and most networked computers, this provides a simpler installation. Modbus TCP/IP uses standard Ethernet equipment.

Modbus on UDP

When Sierra Wireless AirLink devices are used in place of radios, a AirLink device is connected to the central station (host) and an AirLink device is connected to each remote unit. When the AirLink device is configured for Modbus with UDP, the AirLink device connected to the host can store a list of IP addresses or names with matching IDs. When the host at the central station sends serial data as a poll request, the AirLink device at the host matches the RTU ID to a corresponding IP of a AirLink device at a remote unit. A UDP packet is assembled encapsulating the RTU ID and serial data transmitted from the host. The UDP packet is then transmitted to the specific AirLink device at the remote unit matching the RTU ID. The remote AirLink device then disassembles the packet before transmitting the RTU ID and serial data to the remote unit. The remote units operate in normal UDP mode and their data is sent to the host via the remote AirLink device and host AirLink device.

Configuring the AirLink Device at the Polling Host for Modbus on UDP

This section covers a Polling Host with standard Modbus, variations may need additional AT commands.

1. Configure the ports.

The destination port for the device at the host needs to match the device port (*DPORT) in use on all the modems at the remote sites. For example, if the remote device's device port (*DPORT) is "12345", then the Modbus host device's *S53* destination port should be set to "12345".

Take note of (or set) the Device Port setting in *DPORT to configure the destination port on the remote modems.

In ACEmanager, select *UDP* in the side menu. Select the appropriate *MD* mode from the drop down menu.

- **MD13**: Modbus ASCII
- **MD23**: Modbus RTU (Binary)
- **MD33**: BSAP
- **MD63**: Variable Modbus — individual parameters are set up manually.

If you do not have a static IP, the host device should be configured to report its current IP to a Dynamic DNS (DDNS) server with Dynamic DNS.

In the Host device's configuration, instead of an IP address for the Addr List (ATMLIST or ATMLISTX), substitute a single unique name for each device, i.e. remote1, remote2, etc.

When you configure Dynamic DNS for the host device, make note of your device name and domain setting in ACEmanager in the menu selection *Dynamic IP* to be used with the remote modems.

With names instead of IP addresses for the Address List, the host device queries the DNS server for the current IP address assigned to the specific name of a remote device to send a message corresponding to the ID.

When you use names instead of IP addresses, to ensure your modems are updated quickly with the correct IP addresses for the names, set the DNS settings as well. In ACEmanager, select *DNS*.

Configure *DNSUSER to the same IP address as the Dynamic DNS (*IPMANAGER1). If your modems have dynamic IP addresses and not static (the IP address can change when it is powered up), configure *DNSUPDATE to a low interval to allow frequent updates.

Configuring the Remote AirLink Devices for Modbus with UDP

This section covers standard Modbus settings for the AirLink device at the remote unit; variations may need additional commands.

1. Configure the ports

In ACEmanager, select Port Configuration in the side menu.

The destination port for the device at the host needs to match the device port in use on all the devices at the remote sites. For example, if the remote device's device port (see below) is "12345", then the Modbus host device's *S53* destination port should be set to "12345".

Set the destination port (S53) to match the device port of the host device (*DPORT). Make sure the device port of the remote device (*DPORT) matches the destination port of the host device (S53).

Configure IP Addresses for the Host

If the Host device has a static IP address, enter it in the Destination Address for S53.

Note: With a name instead of IPs for the host device, the remote devices query the DNS server for the current IP assigned to the host device before sending data back to the host.

If the device at the host has a dynamic IP and is using Dynamic DNS, instead of an IP address for S53, specify the name of the host device (**). If the remote devices are using a different DDNS than the host device, you need to specify the fully qualified domain name (**+*DOMAIN).

*Note: Setting the Host device IP address as the S53 Destination Address provides a low level security. The device does not forward UDP traffic unless the source IP/port matches what is in S53. However, if you set *AIP=1, the device forwards UDP traffic from any source IP address as long as it is accessing the device on the configured *DPORT.*

1. Configure the default mode for start-up.

Each device at the remote locations needs to be configured to communicate with the device at the host. In ACEmanager, select *UDP* in the side menu.

   a. Enable *S82*, UDP auto answer.
   b. Set *S83* to the idle time-out applicable to your application, commonly 20.

2. Configure other RTU settings.

Other parameters may need to be changed, but this is dependent on the RTU type being used. At a minimum, this typically involves setting the proper serial settings to match your RTU.

3. Optional: Dynamic IP Address

If you do not have a static IP, the host device should be configured to report its current IP to a Dynamic DNS (DDNS) server with Dynamic DNS.

Match the name of the device to the names specified in the host device's MLIST or MLISTX for the connected RTU.

When you configure Dynamic DNS for the host device, note your device name and domain setting in ACEmanager in the menu selection *Dynamic IP* to be used with the remote devices.

When you use names instead of IP addresses, to ensure your devices are updated quickly with the correct IP addresses for the names, set the DNS settings as well.

Configure *DNSUSER to the same IP address as the Dynamic DNS (*IPMANAGER1). If your devices have dynamic IP addresses and not static (the IP address can change when it is powered up), configure *DNSUPDATE to a low interval to allow frequent updates.

C: SNMP: Simple Network Management Protocol

C

Management Information Base (MIB)

ALEOS includes a Management Information Base (MIB) that contains information specific to the AirLink device. Reports based on this database are sent in a form designed to be parsed by the NMS. The data is hierarchical with entries addressed through object identifiers.

The MIB complies with:

- RFC 1213 and MIB-II
- RFC 2665 — Ethernet-Like Interface Types
- RFC 2863 — The Interfaces Group MIB

SNMP Traps

SNMP traps are alerts that can be sent from the managed device to the Network Management System when an event happens. Your AirLink device is capable of sending traps when the network connection becomes available.

To send SNMP traps:

1. In ACEmanager, go to Services > Management (SNMP).
2. Configure the fields under Trap Server User. (For more information, see Management (SNMP) on page 220.)
3. Go to Events Reporting > Actions.
4. In the Action Type field select SNMP trap. (For more information, see Action Types on page 260.)
5. Go Events Reporting > Events and configure monitoring for the event type that will trigger the SNMP trap. For example, the event type could be RSSI, thresholds, network state, hardware temperature, etc.

Sierra Wireless MIB

This section show the contents of the Sierra Wireless MIB file. When this file is loaded onto a remote SNMP client, you can query the Sierra Wireless specific objects listed in this file.

For a text copy of this MIB file, go to www.sierrawireless.com/en/Support/Downloads.aspx, and select your AirLink device.

```
SIERRA-MIB DEFINITIONS ::= BEGIN

IMPORTS
   OBJECT-TYPE, NOTIFICATION-TYPE, MODULE-IDENTITY, IpAddress,
   Integer32, Opaque, enterprises, Counter32, Unsigned32
      FROM SNMPv2-SMI

   TEXTUAL-CONVENTION, DisplayString, TruthValue
FROM SNMPv2-TC;

sierrawireless MODULE-IDENTITY
   LAST-UPDATED "201202290000Z"
   ORGANIZATION "Sierra Wireless Inc"
   CONTACT-INFO
"Sierra Wirelss Inc
      "

   DESCRIPTION
""
   REVISION "201202290000Z"

   DESCRIPTION
"This file defines the private Sierra MIB extensions."

   ::= { enterprises 20542 }

sharks OBJECT IDENTIFIER ::= { sierrawireless  9}

-- MIB versions

mibversion1 OBJECT IDENTIFIER ::= { sharks  1}

--  GUI Tabs for Sharks

statustab OBJECT IDENTIFIER ::= { mibversion1  1}
cellulartab OBJECT IDENTIFIER ::= { mibversion1  2}
lantab OBJECT IDENTIFIER ::= { mibversion1  3}
vpntab OBJECT IDENTIFIER ::= { mibversion1 4}
securitytab OBJECT IDENTIFIER ::= { mibversion1  5}
servicestab OBJECT IDENTIFIER ::= { mibversion1  6}
gpstab OBJECT IDENTIFIER ::= { mibversion1  7}
eventsreportingtab OBJECT IDENTIFIER ::= { mibversion1  8}
serialtab OBJECT IDENTIFIER ::= { mibversion1  9}
iotab OBJECT IDENTIFIER ::= { mibversion1  10}
admintab OBJECT IDENTIFIER ::= { mibversion1  11}
snmpconfig OBJECT IDENTIFIER ::= { mibversion1  12}

--  status elements

home   OBJECT IDENTIFIER ::= { statustab  1}
cellular OBJECT IDENTIFIER ::= { statustab  2}
lan  OBJECT IDENTIFIER ::= { statustab  3}
```

```
vpn    OBJECT IDENTIFIER ::= { statustab  4}
security    OBJECT IDENTIFIER ::= { statustab  5}
services    OBJECT IDENTIFIER ::= { statustab  6}
gps    OBJECT IDENTIFIER ::= { statustab  7}
serial    OBJECT IDENTIFIER ::= { statustab  8}
about    OBJECT IDENTIFIER ::= { statustab  9}


-- home status elements

phoneNumber OBJECT-TYPE
SYNTAX DisplayString (SIZE (10))
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 17 }

ipAddress OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 301 }

networkState OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 259 }

rssi OBJECT-TYPE
SYNTAX INTEGER(-125..-50)
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 261 }

gprsnetworkOperator OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 770 }

cdmanetworkOperator OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 644 }
```

```
gprsECIO OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
 DESCRIPTION ""
::= { home 772 }

cdmaECIO OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
  DESCRIPTION ""
::= { home 643 }

powerIn OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 266 }

boardTemprature OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 267 }

networkServiceType OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 264}

aleosSWVer OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 4 }

netChannel OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 260 }

cellularBytesSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
```

```
STATUS current
   DESCRIPTION ""
::= { home 283 }

cellularBytesRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 284 }


deviceName OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 1154 }

-- cellular status elements

wanIP OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 301 }

electronicID OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 10 }

iccid OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 771 }

cellid OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 773 }

lac OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
```

```
STATUS current
   DESCRIPTION ""
::= { cellular 774 }

imsi OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 785 }

keepAliveIpAddress OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 1105 }

keepAlivePingTime OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 1104 }

dnsServer1 OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 1082 }

dnsServer2 OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 1083 }

cellBand OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 2056 }

apn OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 2151 }
```

```
wanUseTime OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 5046 }

rscp OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 10249 }

errorRate OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 263 }

bytesSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 283 }

bytesRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 284 }

packetsSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 281 }

packetsRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 282 }

prlVersion OBJECT-TYPE
SYNTAX INTEGER
```

```
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 642 }

prlUpdateStatus OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 646 }

sid OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 648 }

nid OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 649 }

pnOffset OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 650 }

baseClass OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 651 }

-- LAN status elements

usbMode OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 1130 }

vrrpEnabled OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
```

```
STATUS current
   DESCRIPTION ""
::= { lan 9001 }

lanpacketsSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 279 }

lanpacketsRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 280 }

wifipacketsSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 10405 }

wifipacketsRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 10406 }

wifiBridgeEnabled OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 10401 }

wifiSecurityType OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 4509 }

wifiAPStatus OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 4506 }
```

```
wifiSSID OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 4507 }

wifiChannel OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 4508 }

-- VPN status elements


incomingOOB OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { vpn 3177 }

outgoingOOB OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { vpn 3178 }

outgoingHostOOB OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { vpn 3179 }


vpn1Status OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { vpn 3176 }

vpn2Status OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
```

```
::= { vpn 3205 }

vpn3Status OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { vpn 3231 }

vpn4Status OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { vpn 3257 }

vpn5Status OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { vpn 3283 }

-- Security status elements

dmz OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 5113 }

portForwarding OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 5112 }

portFilteringIn OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 3505 }

portFilteringOut OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 3506 }
```

```
trustedHosts OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 1062 }

macFiltering OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 3509 }

badPasswdCount OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 385 }

ipRejectCount OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 386 }

ipRejectLog OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 387 }

-- Services status elements

aceNet OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { services 5026 }

aceManager OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { services 1149 }
```

```
dynamicDnsService OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { services 5011 }

fullDomainName OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { services 5007 }

-- GPS status elements

gpsFix OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 900 }

satelliteCount OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 901 }

latitude OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 902 }

longitude OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 903 }

heading OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 904 }

speed OBJECT-TYPE
```

```
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 905 }

engineHours OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 906 }

-- Serial status elements

serialPortMode OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { serial 1043 }

tcpAutoAnswer OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { serial 1048 }

udpAutoAnswer OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { serial 1054 }

serialPacketsSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { serial 273 }

serialPacketsRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { serial 274 }

-- About status elements
```

```
deviceModel OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 7 }


radioModelType OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 9 }

radioFirmwareVersion OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 8 }

deviceID OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 25 }

macAddress OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 66 }

aleosSWVersion OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 4 }

deviceHwConfiguration OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 5 }

msciVersion OBJECT-TYPE
SYNTAX DisplayString
```

```
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 3 }

-- Read Write values

snmpenable OBJECT-TYPE
SYNTAX INTEGER {
       disabled(0),
       enabled(1)}
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10040 }

snmpversion OBJECT-TYPE
SYNTAX INTEGER {
       snmpv2c(2),
       snmpv3(3)}
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10041 }

snmpport OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10042 }

snmpContact OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  2730 }

snmpName OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  2731 }

snmpLocation OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  2732 }
```

```
rocommunity OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10063 }

rouser OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10045 }

rosecuritylvl OBJECT-TYPE
SYNTAX INTEGER {
       noauthnopriv(0),
       authnopriv(1),
       authpriv(2)}
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10046 }

roauthtype OBJECT-TYPE
SYNTAX INTEGER {
       md5(0),
       sha(1) }
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10047 }

roauthkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10048 }

roprivtype OBJECT-TYPE
SYNTAX INTEGER {
       aes(0),
       des(1) }
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10049 }

roprivkey OBJECT-TYPE
SYNTAX DisplayString
```

```
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10050 }


rwcommunity OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10064 }

rwuser OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10051 }

rwsecuritylvl OBJECT-TYPE
SYNTAX INTEGER {
       noauthnopriv(0),
       authnopriv(1),
       authpriv(2)}
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10052 }

rwauthtype OBJECT-TYPE
SYNTAX INTEGER {
       md5(0),
       sha(1) }
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10053 }

rwauthkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10054 }


rwprivtype OBJECT-TYPE
SYNTAX INTEGER {
       aes(0),
       des(1) }
MAX-ACCESS read-write
```

```
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10055 }

rwprivkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10056 }


trapipAddress OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 1166 }

trapport OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10043 }

engineid OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10044 }

trapcommunity OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10065 }

trapuser OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10057 }

trapsecuritylvl OBJECT-TYPE
SYNTAX INTEGER {
       noauthnopriv(0),
       authnopriv(1),
       authpriv(2)}
```

```
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10058 }

trapauthtype OBJECT-TYPE
SYNTAX INTEGER {
       md5(0),
       sha(1) }
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10059 }

trapauthkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10060 }


trapprivtype OBJECT-TYPE
SYNTAX INTEGER {
       aes(0),
       des(1) }
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10061 }

trapprivkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10062 }


rebootmodem OBJECT-TYPE
SYNTAX INTEGER {
       nop(0),
       reboot(1) }
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 65001 }



-- Notifications starting at 1000
```

```
modemNotifications OBJECT IDENTIFIER ::= { mibversion1  1000 }


value OBJECT-TYPE
   SYNTAX      DisplayString
   MAX-ACCESS  accessible-for-notify
   STATUS      current
   DESCRIPTION
      "value of MSCIID that triggered this event"
::= { modemNotifications 500 }

digitalInput1 NOTIFICATION-TYPE
   OBJECTS     { value }
   STATUS      current
   DESCRIPTION
      "Digital Input 1 MSCIID 851"
::= { modemNotifications 1 }


digitalInput2 NOTIFICATION-TYPE
   OBJECTS     { value }
   STATUS      current
   DESCRIPTION
      "Digital Input 1 MSCIID 852"
::= { modemNotifications 2 }

digitalInput3 NOTIFICATION-TYPE
   OBJECTS     { value }
   STATUS      current
   DESCRIPTION
      "Digital Input 1 MSCIID 853"
::= { modemNotifications 3 }

digitalInput4 NOTIFICATION-TYPE
   OBJECTS     { value }
   STATUS      current
   DESCRIPTION
      "Digital Input 1 MSCIID 854"
::= { modemNotifications 4 }

pulseAccumulator1 NOTIFICATION-TYPE
   OBJECTS     { value }
   STATUS      current
   DESCRIPTION
      "Pulse Accumulator 1 MSCIID 4002"
::= { modemNotifications 5 }


pulseAccumulator2 NOTIFICATION-TYPE
   OBJECTS     { value }
   STATUS      current
   DESCRIPTION
```

```
        "Pulse Accumulator 2 MSCIID 4003"
::= { modemNotifications 6 }

pulseAccumulator3 NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Pulse Accumulator 3 MSCIID 4004"
::= { modemNotifications 7 }

pulseAccumulator4 NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Pulse Accumulator 1 MSCIID 4005"
::= { modemNotifications 8 }

analogInput1 NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Analog  Input 1 MSCIID 855"
::= { modemNotifications 9 }


analogInput2 NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Analog  Input 2 MSCIID 856"
::= { modemNotifications 10 }

analogInput3 NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Analog  Input 3 MSCIID 857"
::= { modemNotifications 11 }

analogInput4 NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Analog  Input 4 MSCIID 858"
::= { modemNotifications 12 }

scaledAnalogInput1 NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Scaled Analog  Input 1 MSCIID 4041"
::= { modemNotifications 13 }
```

```
scaledAnalogInput2 NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Scaled Analog  Input 2 MSCIID 4042"
::= { modemNotifications 14 }

scaledAnalogInput3 NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Scaled Analog  Input 3 MSCIID 4043"
::= { modemNotifications 15 }

scaledAnalogInput4 NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Scaled Analog  Input 4 MSCIID 4044"
::= { modemNotifications 16 }

gpsFixNotification NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "GPS Fix MSCIID 900"
::= { modemNotifications 17 }

vehicleSpeed NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Vehicle Speed MSCIID 905"
::= { modemNotifications 18 }

engineHoursNotification NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Engine Hours MSCIID 906"
::= { modemNotifications 19 }

headingChange NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Heading Change MSCIID 904"
::= { modemNotifications 20 }

rssiNotification NOTIFICATION-TYPE
```

```
    OBJECTS    { value }
    STATUS     current
    DESCRIPTION
       "RSSI MSCIID 261"
::= { modemNotifications 21 }

networkStateNotification NOTIFICATION-TYPE
    OBJECTS    { value }
    STATUS     current
    DESCRIPTION
       "Network State MSCIID 259"
::= { modemNotifications 22 }

networkService NOTIFICATION-TYPE
    OBJECTS    { value }
    STATUS     current
    DESCRIPTION
       "Network Service 264"
::= { modemNotifications 23 }

networkErrorRate NOTIFICATION-TYPE
    OBJECTS    { value }
    STATUS     current
    DESCRIPTION
       "Network Error Rate MSCIID 263"
::= { modemNotifications 24 }

periodicReports NOTIFICATION-TYPE
    OBJECTS    { value }
    STATUS     current
    DESCRIPTION
       "Periodic Reports MSCIID 270"
::= { modemNotifications 25 }

powerInNotification NOTIFICATION-TYPE
    OBJECTS    { value }
    STATUS     current
    DESCRIPTION
       "Power In  MSCIID 266"
::= { modemNotifications 26 }

boardTemp NOTIFICATION-TYPE
    OBJECTS    { value }
    STATUS     current
    DESCRIPTION
       "Board Temperature MSCIID 267"
::= { modemNotifications 27 }

cdmaTemp NOTIFICATION-TYPE
    OBJECTS    { value }
    STATUS     current
    DESCRIPTION
```

```
      "CDMA Temperature MSCIID 641"
::= { modemNotifications 28 }


dailyDataUsage NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Daily Data Usage MSCIID 25001"
::= { modemNotifications 29 }

monthlyDataUsage NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Monthly Data Usage MSCIID 25002"
::= { modemNotifications 30 }

END
```

D: AT Commands

AT Command Set Summary

Using a terminal connection (Telnet) or SSH protocol, you can send AT commands to configure the device, command it to do something, or query a setting.

- AT commands must always be terminated by a carriage return <CR> (ASCII character 0x0D), i.e., pressing enter on the keyboard. Some may also include a new line or line feed <LF>.
- If **E=1** (Echo On), the AT command (including the terminating <carriage return>) is displayed (output) before any responses.
- Two settings affect the format of AT command output: V (Verbose) and Q (Quiet).
- If Q=1 (Quiet On), no result codes are output whatsoever, so there is no response generated by a (non-query) command.
- If Q=0 (Quiet Off), result codes are output. The format of this output is then affected by the Verbose setting.

  If Quiet mode is off, the result code is affected as follows:

  For V=1 (Verbose mode), the textual result code is surrounded by a carriage return and new line. Any AT query response is also surrounded by a carriage return and new line.

  For V=0 (Terse mode), a numeric result code is output with a single trailing carriage return (no new line is output), while any AT query response is followed by a carriage return and new line (there is no preceding output).
- For example, possible output to the AT command “AT” with carriage return (assuming quiet mode is not on) is:

  carriage return — if V=0

  carriage return and new line OK another carriage return and new line — if V=1

Note: AT commands work for the port on which they are executed. For example, if the user types ATE1 and then AT&W using a USB/serial port connection, it sets the USB/serial port to Echo On but not the telnet connection or the RS232 serial port.

If you need to change the port for Telnet (for example, you have the default port blocked on your firewall), the option is on the Services > Telnet/SSH tab. The default Telnet port is 2332. You can also change the Telnet timeout; if the connection is idle, default timeout is 2 minutes. This is the internal Telnet on the device to pass AT commands and not TCP PAD.

AT commands are shown in upper case, but they are not case sensitive.

This appendix organizes the commands into functional groups to allow you to more quickly locate a desired command when you know the operation but not the command. Commands under each topic are listed alphabetically.

Note: Some of the configuration commands listed here are only available as AT commands.

Reference Tables

Result codes are not shown in the command tables unless special conditions apply. Generally the result code OK is returned when the command has been executed. ERROR may be returned if parameters are out of range, and is returned if the command is not recognized or is not permitted in the current state or condition of the AirLink device.

Note: Unless otherwise stated, all commands are accessible locally and remotely.

AT command topics in this appendix:

- Standard (Hayes) commands on page 436
- Device Updates on page 389
- Status on page 389
- WAN/Cellular on page 395
- LAN on page 401
- Wi-Fi on page 403
- VPN on page 407
- Security on page 412
- Services on page 413
- GPS on page 422
- Serial on page 429
- I/O on page 442
- Applications on page 443
- Admin on page 444

Device Updates

Table D-1: Device Update AT Commands

Command	Description
***TPLUPDATE**	This AT command updates the template (configuration file) remotely. The template file must be accessible on an FTP server. The command parameters are: AT*TPLUPDATE=<Server_IP>,<USER_NAME>,<PASSWORD>,<FILE_NAME> where: • SERVER_IP is the IP address of the FTP server. • USER_NAME is the user name used to access the FTP server. • PASSWORD is the password used to access the FTP server. • FILE_NAME is the name of the template file on the FTP server that you want to apply to the AirLink device. The template file must be stored on the FTP User_Name home, not in a sub-folder. Example: AT*TPLUPDATE=192.168.17.111,MyUserName,MyPassword,NewTemplate.xml When the template is successfully applied, the message displayed is: `Template applied successfully` OK *Note: Configure the FTP server:* • *As passive mode (not active mode)* • *To listen to port 21*

Status

Table D-2: Status AT Commands

Command	Description
***BAND?**	HSPA and LTE fallback to HSPA only. Query the current radio module band.
***CELLINFO?**	Query cellular connection information.
***CELLINFO2?**	Query in depth cell information.
+CIMI?	HSPA and LTE only. Query the IMSI.

Table D-2: Status AT Commands (Continued)

Command	Description
***DEVICEID?**	When the device is configured to use the device ID with GPS reports, this command displays the 64-bit device ID created from the ESN/IMEI or phone, preceded by the hex delimiter (0x). For example: at*deviceid? 0x010112DE140B5A32 *Note: If the device is not configured to use the device ID with GPS reports, the command returns "NOT SET".*
***DNS1?** ***DNS2?**	Query the primary DNS (*DNS1) and secondary (*DNS2) IP addresses. AT*DNS1? to query DNS1 AT*DNS2? to query DNS2
***DNS1V6?** ***DNS2V6?**	AirLink GX440 only Query the primary IPv6 DNS (*DNS1V6) and secondary (*DNS2V6) IP addresses. AT*DNS1V6? to query DNS1V6 AT*DNS2V6? to query DNS2V6
+ECIO?	Query the signal quality.
***ETHMAC?**	Query the MAC address of the Ethernet port • AT*ETHMAC? or AT*ETHMAC?1— Returns the MAC address of the main Ethernet port If you have a GX Series device with a Dual Ethernet X-Card installed: • AT*ETHMAC?2 — Returns the MAC address of the Ethernet X-Card port marked eth2 • AT*ETHMAC?3 — Returns the MAC address of the Ethernet X-Card port marked eth3
***ETHSTATE?**	Query the connection state (speed and duplex) of the Ethernet port. • AT*ETHSTATE? or AT*ETHSTATE?1— Returns the speed and duplex state of the main Ethernet port (e.g. 100Mb/s Full Duplex) If you have a GX Series device with a Dual Ethernet X-Card installed: • AT*ETHSTATE?2 — Returns the speed and duplex state of the Ethernet X-Card port marked eth2 • AT*ETHSTATE?3 — Returns the speed and duplex state of the Ethernet X-Card port marked eth3
***GLOBALID?**	Query the global ID used by AVMS to identify the device.
***HOSTCOMMLVL?**	Query the serial host signal level. Response example: DCD:LOW; DTR:LOW; DSR:HIGH; CTS:HIGH; RTS:LOW
+HWTEMP?	Query the internal temperature of the radio module (in degrees Celsius).
I[n]	Query device information. • n omitted—device model • n=0—device model • n=1—ALEOS software version, hardware revision, boot version • n=2—Radio module firmware version • n=3—Radio module's unique ID (ESN, IMIEI, or EID)

Table D-2: Status AT Commands (Continued)

Command	Description
+ICCID?	HSPA and LTE only. Query the SIM ID.
***LTERSRQ?**	LTE only Query the LTE signal quality (in dB). For more information, see LTE Signal Quality (RSRQ) on page 47.
***LTERSRP?**	LTE only Query the LTE signal strength (in dBm). For more information, see LTE Signal Quality (RSRQ) on page 47.
***NETCHAN?**	Query the current cellular network channel.
***NETCONNTYPE?**	AirLink GX440 only Query the current IP address type AT*NETCONNTYPE? • 0—None • 1—IPv4 • 3—Both IPv4 and IPv6 gateway *Note: To set the IP address type preference, see *NETIPPREF on page 399.*
NETIP?	Query the current WAN IP address of the device reported by the internal module (generally obtained from your Mobile Network Operator). If the device is connected in Wi-Fi Client mode, the Wi-Fi IP address is returned. If you have an Internet-routable IP address, you can use this address to contact devices from the Internet. If your device uses a different WAN (such as a Wi-Fi client) or is on a private cellular network, you can use this address to contact the device from another host on the same WAN network. If required, use AT**NETALLOWZEROIP to allow displaying an IP address ending in a zero. *Note: If there is no current network IP address, 0.0.0.0 is returned.*
***NETIPV6?**	AirLink GX440 only Query the current IPv6 network IP address of the device reported by the internal module (generally obtained from your Mobile Network Operator). If you have an Internet-routable IP address, you can use this address to contact devices from the Internet. If your device is on a private cellular network, you can use this address to contact the device from another host on the same WAN network. *Note: If there is no current network IPv6 address, "::" (two colons) is returned.*
***NETIPV6PREFIXLEN?**	AirLink GX440 only Query the length of the network IPv6 prefix AT*NETIPV6PREFIXLEN? If there is no IPv6 connection, 0 is returned.

Table D-2: Status AT Commands (Continued)

Command	Description
***NETOP?**	Query the Mobile Network Operator of the active connection. If you are roaming, the roaming operator is returned, if the home operator allows this.
***NETPHONE?**	Query the device's cellular phone number, if applicable or obtainable.
***NETRSSI?**	Query the current RSSI (Receive Signal Strength Indicator) for non-LTE cellular connections, as a negative dBm value.
***NETSERV?**	Query the current connection type (e.g., LTE, HSPA+, EV-DO Rev A, etc.).
***NETSERVICE_RAW?**	Query the numeric value for the network service type. • 8—2G (1x, EDGE, GPRS) • 10—2G roaming • 16—3G (EV-DO Rev. A, HSPA, HSPA+, UMTS) • 18—3G roaming • 64—4G

Table D-2: Status AT Commands (Continued)

Command	Description
***NETSTATE?**	Query the network state of the current WAN connection. AT*NETSTATE? returns: • Connecting To Network—The device is in the process of trying to connect to the cellular network. • Network Authentication Fail—Authentication to the cellular network has failed. Verify settings to activate the device. • Data Connection Failed—The device failed to connect, and it is now waiting a set time interval before it attempts to reconnect. Verify settings to activate the device. • Network Negotiation Fail—Network connection negotiation failed. This is usually temporary and often clears up during a subsequent attempt. • Network Ready—The device is connected to the 1x cellular network and ready to send data. • Network Ready - Wi-Fi—The device is connected to a Wi-Fi network in client mode. • Network Dormant—The device is connected to the 1x cellular network, but the link is dormant. It will be woken up when data is sent or received. • No Service—There is no cellular network detected. • Hardware Reset—The internal module is being reset. This is a temporary state. • No SIM or Unexpected SIM status—No SIM, SIM installed incorrectly, or another SIM error. • Awaiting Provisioning—An EV-DO device without an account and hasn't had an account or the provisioning has been erased from the radio. • Provisioning... —An EV-DO device in the process of writing the account data to the radio. • Not Connected-Waiting for Activity — “Always On Connection” has been disabled and the device is waiting for outgoing traffic or an SMS Wakeup command to mount the PDP context. (This status applies only to OpenSIM devices.) • Not Connected-Radio Connect off—The RADIO_CONNECT AT command was entered, and the PDP context is manually disabled. (This status applies only to OpenSIM devices.) • SIM Locked, but bad SIM PIN. • SIM PIN incorrect 3 attempts left. • SIM PIN incorrect 2 attempts left. • SIM PIN incorrect 1 attempts left. • SIM PIN incorrect 0 attempts left. • SIM Blocked, Bad unlock code. • SIM Blocked, unblock code incorrect.

Table D-2: Status AT Commands (Continued)

Command	Description
***NETSTATE_RAW?**	Query numeric value of the network state of the current WAN connection: • 1—Connecting To Network—The device is in the process of trying to connect to the cellular network. • 4—Network Access Denied—Connection rejected. • 5—Network Ready—WAN is using cellular and is online. • 7—No Service—The WAN link is down or unavailable • 9—No SIM or Unexpected SIM status—No SIM, SIM installed incorrectly, or another SIM error. • 11—Awaiting Provisioning—An EV-DO device without an account and hasn't had an account or the provisioning has been erased from the radio. • 12—Data Connection Failed - Waiting to Retry—The device failed to connect, and it is waiting a set time interval before it attempts to reconnect. Or • 12—Provisioning... —An EV-DO device in the process of writing the account data to the radio. • 13—SIM Locked, but bad SIM PIN. • 14—SIM PIN incorrect 3 attempts left. • 15—SIM PIN incorrect 2 attempts left. • 16—SIM PIN incorrect 1 attempts left. • 17—SIM PIN incorrect 0 attempts left. • 18—SIM Blocked, Bad unlock code. • 19—SIM Blocked, unblock code incorrect. • 27—Network Ready - Wi-Fi—WAN is using Wi-Fi Client and is connected. • 30—Not Connected-Waiting for Activity — “Always On Connection” has been disabled and the device is waiting for outgoing traffic or an SMS Wakeup command to mount the PDP context. (This status applies only to OpenSIM devices.) • 31—Not Connected-Radio Connect off—The RADIO_CONNECT AT command was entered, and the PDP context is manually disabled. (This status applies only to OpenSIM devices.)
+PRL?	CDMA and LTE fallback to EV-DO only Query CDMA Preferred Roaming List (PRL) version.
***PRLSTATUS?**	CDMA only Query the status of the most recent PRL update. • n=0—None (No update) • n=1—In progress • n=2—Update successful The return of any other value indicates that the update failed.
***USBNETSTATE?**	Query the status of the USB connection. AT*USBNETSTATE? returns: • None—There are no USB connections to the AirLink device. • 8 MB/s Half Duplex—There is a USB connection to the device.
***WANUPTIME?**	Query the time in minutes from which the cellular IP is obtained from the mobile network. AT*WANUPTIME?

WAN/Cellular

A reboot is required before the WAN/Cellular AT Commands described in the following table take effect.

Table D-3: WAN/Cellular AT Commands

Command	Description
***AUTOPRL**	CDMA only. Query or set automatic Preferred Roaming List updates AT*PRL? to query AT*PRL=n to set • n=0—Disable • n=1—Enable *Note: To query the current PRL, use +PRL?.*
***AUTOPRLFREQ**	CDMA only. Query or set how often the PRL automatically updates. AT*AUTOPRLFREQ? to query AT*AUTOPRLFREQ=n to set • n= interval to check for updates (in days)
!BAND	HSPA and LTE fallback to HSPA only. Query or set the RF band range or technology. AT!BAND? to query a value sent since the device was last rebooted. AT!BAND=hh to set at the next reboot. • hh=00—All bands • hh=03—GSM 900/1800 • hh=05—GSM All • hh=08—WCDMA All • hh=10—WCDMA 900/2100 *Note: To query the current band, use *BAND?.* *Note: For some Mobile Network Operator SIM Cards, you may need to set the radio band before installing the SIM card.*

Table D-3: WAN/Cellular AT Commands

Command	Description
+CGDCONT	HSPA only Query or set the PDP context, APN, and other information required to establish a connection to o an HSPA network. You only need to configure this once. The parameters are saved and used each time a connection is made to the HSPA network. AT+CGDCONT? to query AT+CGDCONT = PID,PDP_TYPE,APN [,IPADDR] to set PID= PDP context identifier PDP_TYPE = numeric parameter that specifies a PDP context definition APN = Access Point Name IPADDR = IP address Examples: AT+CGDCONT=1,IP,proxy AT+CGDCONT=1,IP,internet *Note: When using the APN-related optons in ACEmanager, you generally do not need to configure +CGDCONT.*
***CLIENT_PPP_AUTH**	Query or set the Force Network Authentication mode. AT*CLIENT_PPP_AUTH? to query AT*CLIENT_PPP_AUTH=n to set • n=0—None • n=1—PAP • n=2—CHAP
+COPS	HSPA only Query or set the network operator and the connection mode. AT+COPS? to query AT+COPS=MODE[,FORMAT[,OPER]] to set MODE • MODE=0 — Automatic (default) • MODE= 1 — Manual • MODE=4 — Manual/Automatic; if manual failed, it defaults to automatic FORMAT • FORMAT=0 — Alphanumeric (“Name”) • FORMAT=2 — Numeric OPER • OPER= the operator numeric code Example, AT+COPS=1,2,302610 Manual mode, numeric format, operator code 302610 *Note: On some cellular networks, explicit use of +COPS allows you to select the roaming Mobile Network Operator to use.*

Table D-3: WAN/Cellular AT Commands

Command	Description
***EVDODATASERV**	CMDA and LTE fallback to EV-DO only. Query or set the allowable network type. AT*EVDODATASERV? to query AT*EVDODATASERV=n to set • n=0 — EV-DO Preferred — can “fall back” on CDMA/1x (only available on EV-DO devices) • n=0 — LTE Preferred — can “fall back” on CDMA/EV-DO (only available on LTE devices) • n=1 — EV-DO Only — fall back disabled (only available on 1x/EV-DO devices) • n=2 — 1x Only — EV-DO disabled (only available on 1x/EV-DO devices) • n=3—CDMA Only — LTE disabled (only available on LTE devices) • n=4—LTE Only — Fall back disabled (only available on LTE devices) *Note: If you choose one of the options where fall back is disabled and the selected network type is not available, the device will not be able to connect to the cellular network. For example, if you select LTE Only and you are in an area where there is no LTE network available, the device will not be able to connect to a cellular network until you change this setting or move to an area with LTE coverage.*
***EVDODIVERSITY**	CDMA only. For HSPA device, see *RXDIVERSITY on page 400. Query or set EV-DO Diversity, which allows two antennas to provide more consistent connection. AT*EVDODIVERSITY? to query AT*EVDODIVERSITY=n to set • n=0 — Disabled • n=1 — Enabled *Note: If you are not using a diversity antenna, *EVDODIVERSITY should be disabled.*
***EVDOROAMPREF**	CDMA and LTE fallback to EV-DO only Query or set the network roaming preference AT*EVDOROAMPREF? to query AT*EVDOROAMPREF=n to set • n=0—Automatic • n=1—Home only
***HANGUPTORESET**	HSPA only. Query or set forcing the radio module to reset when the device disconnects. AT*HANGUPTORESET? to query AT*HANGUPTORESET=n to set • n=0—Disable • n=1—Enable

Table D-3: WAN/Cellular AT Commands

Command	Description
***IPPING**	Query or set the interval between keepalive pings (in minutes) if no valid packets have been received by the IP address or FQDN specified in *IPPINGADDR. AT*IPPING? to query the Keepalive PING time interval AT*IPPING=n to set the Keepalive PING time interval • n=0 — Disable pinging (default) • n=15–255 minutes *Note: 15 minutes is the minimum interval for Keep Alive. If you set *IPPING for a value between 0 and 15, the idle interval for pings will be 15 minutes.*
***IPPINGADDR**	Query or set the Keepalive PING IP address or FQDN for the device to ping when Keepalive Ping Time (*IPPING) is set. AT*IPPINGADDR? to query AT*IPPINGADDR=[d.d.d.d] or [n] • d.d.d.d=IP address • n=domain name *Note: AT*IPPING must to be set to a value other than 0 to enable pinging.*
***IPPINGFORCE**	Query or set the Force Keepalive Ping setting. When this feature is enabled, the Keepalive ping is sent even if IP traffic has occurred during the configured interval. AT*IPPINGFORCE? to query AT*IPPINGFORCE=n to set • n=0—Disable • n=1—Enable *Note: To enable this command, *IPPING must be enabled and *IPPINGADDR configured.*
***NETALLOWZEROIP**	Query or set allowing the device to get an IP address from the cellular network that has the last octet as 0 (zero). AT*NETALLOWZEROIP? to query AT*NETALLOWZEROIP=n to set • n=0 — Do not allow • n=1 — Allow Allows the device to use a WAN IP address that ends in zero (e.g. 192.168.1.0).
***NETAPN**	HSPA and LTE fallback to HSPA only Query or set the user entered APN. AT*NETAPN? to query AT*NETAPN=APN to set (up to 80 characters) *Note: When you set this command, the APN type is automatically set to User Entry so that the APN you enter with this AT command is used on reboot.*

Table D-3: WAN/Cellular AT Commands

Command	Description
***NETIPPREF**	AirLink GX440 only Query or set the IP Address Preference. *Note: To use IPv6, it must be supported by your Mobile Network Operators and your account (SIM and APN).* AT*NETIPPREF? to query AT*NETIPPREF=n to set • n=0—IPv4 • n=1—IPv4 and IPv6 Gateway *Note: To determine the current network IP type, see *NETCONNTYPE? on page 391.*
***NETPW**	Set the cellular network account password, if required. AT*NETPW=PW to set (up to 30 characters) *Note: AT*NETPW? returns a dotted display for privacy.*
***NETUID**	Query or set the cellular network account user ID, if required. AT*NETUID? to query AT*NETUID=USER ID (up to 64 bytes)
***NWDOG**	Query or set the interval that the network connection watchdog waits for a network connection. If no connection is established within this interval, the device resets. AT*NWDOG? to query AT*NWDOG=n to set • n=0—Disable • n=1—5 Minutes • n=2—10 Minutes • n=3—15 Minutes • n=4—30 Minutes • n=5—45 Minutes • n=6—1 Hour • n=7—2 Hours (default) • n=8—3 Hours • n=9—4 Hours
PING	Sends 5 PING to a single address. Returns OK if there is a response: ERROR if there is no response. ATPING[ip address or FQDN] *Note: Do not use an equal sign (=) when issuing the command.* Example: ATPINGsierrawireless.com

Table D-3: WAN/Cellular AT Commands

Command	Description
$QCMIP	CDMA and LTE fallback to EV-DO only Query or set use of Mobile IP (MIP) preferences. $QCMIP? to query $QCMIP=n to set • n=0—Disabled, Simple IP (SIP) only • n=1—Mobile IP preferred • n=2—Mobile IP only

***RADIO_CONNECT**	This AT Command applies only to OpenSIM devices on the Vodafone network.
	Query or set the wireless connection setting.
	AT*RADIO_CONNECT? to query
	AT*RADIO_CONNECT=n to set
	• n=0—Disables data traffic. The only way to change this mode is to issue a radio_connect=1 or radio_connect=2 AT command.
	• n=1—Enables Always on connection.
	• n=2—Disables Always on connection. The device listens for outgoing traffic and establishes a mobile network data connection for a specified time:
	  • When there is outgoing traffic
	  or
	  • When it receives a Wakeup SMS, provided Wakeup SMS is configured.
	  (Use *TRAFWUPTOUT on page 401 to set the timeout period.)
	Note: This command is not persistent over device resets.
	Note: You can only send this command locally over a serial, serial USB, or local telnet/SSH connection.

***RADIO_CONNECT_ STARTUP**	This AT Command applies only to OpenSIM devices on the Vodafone network. You can query this command remotely or locally, but it can only be set locally. This command is the same as *RADIO_CONNECT, except • The change does not take effect until the next reboot. • The setting is persistent over subsequent reboots.
***RXDIVERSITY**	HSPA only. For CDMA devices, see *EVDODIVERSITY on page 397. Query or set the RX Diversity setting. Rx Diversity allows you to use two antennas for a more consistent connection. If you are not using a diversity antenna, Rx Diversity should be disabled. AT*RXDIVERSITY? to query AT*RXDIVERSITY=n to set • n=0—Disable • n=1—Enable *Note: This AT Command is not available for all AirLink devices.*

Table D-3: WAN/Cellular AT Commands

Command	Description
***SIMPIN**	HSPA and LTE fallback to HSPA only Query or enter the SIM pin. AT*SIMPIN? to query AT*SIMPIN=n to enter the SIM pin
***SIMPINENABLE**	HSPA and LTE fallback to HSPA only Query or set the SIM pin. AT*SIMPINENABLE? to query AT*SIMPINENABLE=n to set • n=0—Don't change • n=1—Enable (SIM pin required on startup) • n=2—Disable
***TRAFWUPTOUT**	This AT Command applies only to OpenSIM devices on the Vodafone network. Query or set the timeout period after which, if there is no outgoing WAN traffic, the connection is terminated. The timeout period only takes effect if *RADIO_CONNECT or *RADIO_CONNECT_STARTUP is set to 1, or Always on connection is disabled in ACEmanager. (See Always on connection on page 82.) AT*TRAFWUPTOUT? to query AT*TRAFWUPTOUT=n to set • n=2–65535 minutes (default is 2) *Note: This timer is reset to zero each time a WAN packet goes out.*

LAN/Wi-Fi

LAN

Note: A reboot is required before these commands take effect.

Table D-4: LAN AT Commands

Command	Description
***DHCPHOSTEND**	Query or set the ending IP address for the Ethernet DHCP pool AT*DHCPHOSTEND? to query AT*DHCPHOSTEND=d.d.d.d to set • d.d.d.d=last IP address in Ethernet DHCP pool
***DHCPNETMASK**	Query or set the Ethernet DHCP subnet mask AT*DHCPNETMASK? to query AT*DHCPNETMASK=d.d.d.d to set • d.d.d.d=Ethernet DHCP subnet mask

Table D-4: LAN AT Commands (Continued)

Command	Description
***DHCPSERVER**	Query or set the Ethernet DHCP server. AT*DHCPSERVER? to query AT*DHCPSERVER=n to enable or disable the DHCP server mode • n=0—Disable • n=1—Enable
***DNS1?** ***DNS2?**	Query the primary DNS (*DNS1) and secondary (*DNS2) IP addresses. AT*DNS1? to query DNS1 AT*DNS2? to query DNS2
***DNS1V6?** ***DNS2V6?**	AirLink GX440 only Query the primary IPv6 DNS (*DNS1V6) and secondary (*DNS2V6) IP addresses. AT*DNS1V6? to query DNS1V6 AT*DNS2V6? to query DNS2V6
***DNSUSER**	Query or set the first alternate server for DNS override. (Applies only to primary DNS.) AT*DNSUSER? to query AT*DNSUSER=d.d.d.d • d.d.d.d=IP address of domain server
***HOSTAUTH**	Query or set the Host Authentication mode for PPPoE only. (It does not set host authentication for PPP/DUN.) AT*HOSTAUTH? to query AT*HOSTAUTH=n to set • n=0—None/Disables authentication for PPPoE (default). • n=1— Authentication through PAP • n=2—Authentication through PAP & CHAP
***HOSTPEERIP**	Query or set the IP address of the device's Ethernet port. By default this is 192.168.13.31. *Note: Any connected LAN host can access this IP addresses, whether using a private or public IP address. This IP address must be in the same subnet as the Ethernet DHCP pool.* AT*HOSTPEERIP? to query AT*HOSTPEERIP=d.d.d.d to set • d.d.d.d=local or peer IP address of the device
***HOSTPRIVIP**	Query or set the starting IP for the Ethernet DHCP pool. AT*HOSTPRIVIP? to query AT*HOSTPRIVIP=d.d.d.d to set • d.d.d.d=IP Address

Table D-4: LAN AT Commands (Continued)

Command	Description
***HOSTPRIVMODE**	Query or set the host communication mode used for tethered IP connections. AT*HOSTPRIVMODE? to query AT*HOSTPRIMODE=n to set which user interface uses the Public IP address • n=0—Ethernet Uses Public IP • n=1—All Hosts Use Private IPs • n=2—USB Uses Public IP • n=3—DUN Uses Public IP • n=4—First Host gets Public IP
***HOSTPW**	Query or set the host password for PPPoE only. (It does not set the password for PPP/DUN.) AT*HOSTPW? to query AT*HOSTPW=PASSWORD to set *Note: PASSWORD cannot be "password".*
***HOSTUID**	Query or set the Host user ID for PPPoE only. (It does not set the user ID for PPP/DUN.) AT*HOSTUID? to query AT*HOSTUID=USER ID to set (up to 64 bytes) *Note: USER ID cannot be "user".*
***USBDEVICE**	Query or set the USB Device Mode. This parameter alters the default startup data mode. AT*USBDEVICE? to query AT*USBDEVICE=n to set • n=0—USB Serial • n=1—USBNET • n=2—Disabled

Wi-Fi

Wi-Fi AT Commands are only applicable if the AirLink device has an installed Wi-Fi X-Card and is in Access Point Mode.

Note: You need to configure Client Mode in ACEmanager. There is no AT Command for Wi-Fi Client mode. See Wi-Fi Mode on page 115.

Note: A reboot is required before these commands take effect.

Table D-5: Wi-Fi AT Commands

Command	Description
***APBRIDGED**	Query or set the Bridge Wi-Fi Access Point to Ethernet feature. AT*APBRIDGED? to query AT*APBRIDGED=n to set • n=0 —Disable • n=1 —Enable
***APCHANNEL**	Query or set the Wi-Fi Access Point channel to use. AT*APCHANNEL? to query AT*APCHANNEL=n to set • n = 1 – 11 (available channels)
***APEN**	Query or set the Wi-Fi Access Point mode. AT*APEN? to query AT*APEN=n to set • n=2 —b/g Enabled • n=3 —b/g/n Enabled
***APENDIP**	Query or set the ending IP address for the Wi-Fi Access Point DHCP pool. AT*APENDIP? to query AT*APENDIP=d.d.d.d to set • d.d.d.d= IP Address
***APHOSTIP**	Query or set the Host Wi-Fi Access Point device IP address. AT*APHOSTIP? to query AT*APHOSTIP=d.d.d.d to set • d.d.d.d= IP Address
***APMAXCLIENT**	Query or set the maximum number of Wi-Fi Access Point clients. AT*APMAXCLIENT? to query AT*APMAXCLIENT=n to set • n=0–8
***APNETMASK**	Query or set the Wi-Fi DHCP subnet mask. AT*APNETMASK? to query AT*APNETMASK=d.d.d.d to set • d.d.d.d = IP Address
***APSECURITYTYPE?**	Query the Wi-Fi Access Point Security Encryption type. AT*APSECURITYTYPE? • n=0—Open (WEP encryption) • n=3—WPA Personal • n=5—WPA2 Personal *Note: WEP is not a recommended Wi-Fi Security protocol because of its vulnerabilities and because only alphanumeric characters can be used for the passphrase. Use WPA/WPA2 instead.*

Table D-5: Wi-Fi AT Commands (Continued)

Command	Description
***APSSIDBCAST**	Query or set the broadcast Wi-Fi Access Point SSID. AT*APSSIDBCAST? to query AT*APSSIDBCAST=n to set • n=0 —Disable • n=1 —Enable
***APSSIDVAL**	Query or set the Access Point SSID/Network name. AT*APSSIDVAL? to query AT*APSSIDVAL=n to set • n = ASCII SSID STRING
***APSTARTIP**	Query or set the Query or set the Access Point DHCP start of IP address pool. AT*APSTARTIP? to query AT*APSTARTIP=d.d.d.d to set • d.d.d.d= IP Address
***APTXPWR**	Query or set the Wi-Fi Access Point Transmit Power mode. AT*APTXPWR? to query AT*APTXPWR=n to set • n=0—Low • n=1—Normal
***APWEPENCTYPE?**	Query the Wi-Fi Access Point WEP encryption type. AT*APWEPENCTYPE? • n=0—Disabled (Open) • n=1—WEP *Note: WEP is not a recommended Wi-Fi Security protocol because of its vulnerabilities and because only alphanumeric characters can be used for the passphrase. Use WPA/WPA2 instead.*
***APWEPKEY?**	Query the Wi-Fi Access Point WEB key generated at boot from the WEP passphrase. AT*APWEPKEY?
***APWEPKEYLEN?**	Query the length of the Wi-Fi Access Point WEP key. AT*APWEPKEYLEN? • n=0—64-bit • n=1—128-bit • n=2—Custom
***APWPACRYPT?**	Query the Wi-Fi Access Point WPA/WPA2 encryption type. AT*APWEPKEY? • n=0—TKIP • n=1—AES *Note: If you are using WPA2, only AES is allowed.*

Table D-5: Wi-Fi AT Commands (Continued)

Command	Description
WCC?	Query the Wi-Fi country code.
***WIFIMAC?**	Query the MAC address of the Wi-Fi Access Point. *Note: Wi-Fi Client uses a different MAC address.*
***WIFIMODE**	Query or set the WI-Fi Mode. AT*WIFIMODE? to query AT*WIFIMODE=n to set • n=0—Disabled • n=1—AP (Access Point) • n=2—Client • n=3—AP and Client For more information, see Wi-Fi on page 129.

VPN

Table D-6: VPN Commands

Command	Description
***IPSEC1_AUTH** ***IPSEC2_AUTH** ***IPSEC3_AUTH** ***IPSEC4_AUTH** ***IPSEC5_AUTH**	Query or set the authentication type for # VPN. AT*IPSEC[VPN number]_AUTH? to query AT*IPSEC[VPN number]_AUTH=n to set • n=0 — None • n=1 — MD5 • n=2 — SHA1 (default) • n=3 — SHA 256 *Note: MD5 is an algorithm that produces a 128-bit digest for authentication. SHA is a more secure algorithm that produces both 160-bit (SHA1) and 256-bit (SHA256) digests.*
***IPSEC1_DH** ***IPSEC2_DH** ***IPSEC3_DH** ***IPSEC4_DH** ***IPSEC5_DH**	Query or set how the AirLink Device VPN creates an SA with the VPN server. The DH (Diffie-Hellman) key exchange protocol establishes pre-shared keys during the phase 1 authentication. The AirLink Device supports three prime key lengths, including Group 1 (768 bits), Group 2 (1,024 bits), and Group 5 (1,536 bits). AT*IPSEC[VPN number]_DH? to query AT*IPSEC[VPN number]_DH=n to set • n=0 — None • n=1 — DH1 • n=2 — DH2 (default) • n=5 — DH5
***IPSEC1_ENCRYPT** ***IPSEC2_ENCRYPT** ***IPSEC3_ENCRYPT** ***IPSEC4_ENCRYPT** ***IPSEC5_ENCRYPT**	Query or set the type/length of encryption key used to encrypt/decrypt ESP (Encapsulating Security Payload) packets for # VPN. AT*IPSEC[VPN number]_ENCRYPT? to query AT*IPSEC[VPN number]_ENCRYPT=n to set • n=0 — None • n=1 — DES • n=2 — 3DES • n=3 — AES-128 (default) • n=7 — AES-256 *Note: 3DES supports 168-bit encryption. AES (Advanced Encryption Standard) supports both 128-bit and 256-bit encryption.*
***IPSEC1_GATEWAY** ***IPSEC2_GATEWAY** ***IPSEC3_GATEWAY** ***IPSEC4_GATEWAY** ***IPSEC5_GATEWAY**	Query or set the IP address of the server that # VPN client connects to. AT*IPSEC[VPN number]_GATEWAY? to query AT*IPSEC[VPN number]_GATEWAY=[IP address] to set

Table D-6: VPN Commands (Continued)

Command	Description
***IPSEC1_IKE_AUTH** ***IPSEC2_IKE_AUTH** ***IPSEC3_IKE_AUTH** ***IPSEC4_IKE_AUTH** ***IPSEC5_IKE_AUTH**	Query or set the IKE authentication type for # VPN. AT*IPSEC[VPN number]_IKE_AUTH? to query AT*IPSEC[VPN number]_IKE_AUTH=n to set • n=1 — MD5 • n=2 — SHA1 • n=3 — SHA 256 *Note: MD5 is an algorithm that produces a 128-bit digest for authentication. SHA is a more secure algorithm that produces both 160-bit (SHA1) and 256-bit (SHA256) digests.*
***IPSEC1_IKE_DH** ***IPSEC2_IKE_DH** ***IPSEC3_IKE_DH** ***IPSEC4_IKE_DH** ***IPSEC5_IKE_DH**	Query or set how the AirLink Device VPN creates an SA with the VPN server. The DH (Diffie-Hellman) key exchange protocol establishes pre-shared keys during the phase 1 authentication. The AirLink Device supports three prime key lengths, including Group 1 (768 bits), Group 2 (1,024 bits), and Group 5 (1,536 bits). AT*IPSEC[VPN number]_IKE_DH? to query AT*IPSEC[VPN number]_IKE_DH=n to set • n=1 — DH1 • n=2 — DH2 (default) • n=5 — DH5
***IPSEC1_IKE_ENCRYPT** ***IPSEC2_IKE_ENCRYPT** ***IPSEC3_IKE_ENCRYPT** ***IPSEC4_IKE_ENCRYPT** ***IPSEC5_IKE_ENCRYPT**	Query or set the type/length of IKE encryption key used to encrypt/decrypt ESP (Encapsulating Security Payload) packets for # VPN. AT*IPSEC[VPN number]_IKE_ENCRYPT? to query AT*IPSEC[VPN number]_IKE_ENCRYPT=n to set • n=1 — DES • n=5 — 3DES • n=7 — AES-128 (default) • n=9 — AES-256 *Note: 3DES supports 168-bit encryption. AES (Advanced Encryption Standard) supports both 128-bit and 256-bit encryption.*
***IPSEC1_IKE_LIFETIME** ***IPSEC2_IKE_LIFETIME** ***IPSEC3_IKE_LIFETIME** ***IPSEC4_IKE_LIFETIME** ***IPSEC5_IKE_LIFETIME**	Query or set how long the # VPN tunnel is active (in seconds). AT*IPSEC[VPN number]_IKE_LIFETIME? to query AT*IPSEC[VPN number]_IKE_LIFETIME=n to set • n= 180–86400 • Default is 7200.
***IPSEC1_LIFETIME** ***IPSEC2_LIFETIME** ***IPSEC3_LIFETIME** ***IPSEC4_LIFETIME** ***IPSEC5_LIFETIME**	Query or set how long the # VPN tunnel is active (in seconds). AT*IPSEC[VPN number]_LIFETIME? to query AT*IPSEC[VPN number]_LIFETIME=n to set • n= 180–86400 • Default is 7200.

Table D-6: VPN Commands (Continued)

Command	Description
***IPSEC1_LOCAL_ADDR** ***IPSEC2_LOCAL_ADDR** ***IPSEC3_LOCAL_ADDR** ***IPSEC4_LOCAL_ADDR** ***IPSEC5_LOCAL_ADDR**	Query or set the device subnet address for # VPN. AT*IPSEC[VPN number]_LOCAL_ADDR? returns the device subnet address AT*IPSEC[VPN number]_LOCAL_ADDR=[subnet address] to set
***IPSEC1_LOCAL_ADDR_MASK** ***IPSEC2_LOCAL_ADDR_MASK** ***IPSEC3_LOCAL_ADDR_MASK** ***IPSEC4_LOCAL_ADDR_MASK** ***IPSEC5_LOCAL_ADDR_MASK**	Query or set the device subnet mask information (24-bit netmask) AT*IPSEC[VPN number]_LOCAL_ADDR_MASK? to query AT*IPSEC[VPN number]_LOCAL_ADDR_MASK =[subnet mask] to set Default is 255.255.255.0
***IPSEC1_LOCAL_ADDR_TYPE** ***IPSEC2_LOCAL_ADDR_TYPE** ***IPSEC3_LOCAL_ADDR_TYPE** ***IPSEC4_LOCAL_ADDR_TYPE** ***IPSEC5_LOCAL_ADDR_TYPE**	Query or set the network address type for # VPN. AT*IPSEC[VPN number]_LOCAL_ADDR_TYPE? to query AT*IPSEC[VPN number]_LOCAL_ADDR_TYPE=n to set • n=1 — Use the Host Subnet • n=5 — Single Address • n=17 — Subnet Address (default)
***IPSEC1_LOCAL_ID** ***IPSEC2_LOCAL_ID** ***IPSEC3_LOCAL_ID** ***IPSEC4_LOCAL_ID** ***IPSEC5_LOCAL_ID**	Query or set the local (My Identity) ID for the # VPN. • If IP is selected as the local (My Identity) type, AT*IPSEC[VPN number]_LOCAL _ID? returns the WAN IP address assigned by the Mobile Network Operator • If FQDN or User FQDN is selected as the local (My Identity) type, AT*IPSEC[VPN number]_LOCAL_ID? returns the FQDN (for example me@mycompany.com) To set the local ID: AT*IPSEC[VPN number]_LOCAL _ID=[IP address] or [FQDN], depending on the setting for Local ID (My Identity) type.
***IPSEC1_LOCAL_ID_TYPE** ***IPSEC2_LOCAL_ID_TYPE** ***IPSEC3_LOCAL_ID_TYPE** ***IPSEC4_LOCAL_ID_TYPE** ***IPSEC5_LOCAL_ID_TYPE**	Query or set the local (My Identity) ID type for the # VPN. AT*IPSEC[VPN number]_LOCAL_ID_TYPE? to query AT*IPSEC[VPN number]_LOCAL_ID_TYPE=n to set • n=1 — IP • n=2 — FQDN • n=3 — User FQDN *Note:* • *IP (default) allows you to use an IP address* • *FQDN allows you to use a fully qualified domain name (FQDN) e. g., modemname.domainname.com* • *User FQDN allows you to use a user FQDN whose values should include a username (e.g. user@domain.com)*

Table D-6: VPN Commands (Continued)

Command	Description
***IPSEC1_NEG_MODE** ***IPSEC2_NEG_MODE** ***IPSEC3_NEG_MODE** ***IPSEC4_NEG_MODE** ***IPSEC5_NEG_MODE**	Query or set the negotiation mode for # VPN. AT*IPSEC[VPN number]_NEG_MODE? returns AT*IPSEC[VPN number]_NEG_MODE=n to set • n=1 — Main • n=2 — Aggressive *Note: Aggressive mode offers increased performance at the expense of security.*
***IPSEC1_PFS** ***IPSEC2_PFS** ***IPSEC3_PFS** ***IPSEC4_PFS** ***IPSEC5_PFS**	Query or set the Perfect Forward Secrecy (PFS) setting for # VPN. PFS provides additional security through a DH shared secret value. When this feature is enabled, one key cannot be derived from another. This ensures previous and subsequent encryption keys are secure even if one key is compromised. AT*IPSEC[VPN number]_PFS? to query PFS AT*IPSEC[VPN number]_PFS=n to set PFS • n=0 — Yes (default) • n=1 — No
***IPSEC1_REMOTE_ADDR** ***IPSEC2_REMOTE_ADDR** ***IPSEC3_REMOTE_ADDR** ***IPSEC4_REMOTE_ADDR** ***IPSEC5_REMOTE_ADDR**	Query or set the IP address of the device behind the gateway for # VPN. AT*IPSEC[VPN number]_REMOTE_ADDR? to query AT*IPSEC[VPN number]_REMOTE_ADDR=[IP address] to set
***IPSEC1_REMOTE_ADDR_MASK** ***IPSEC2_REMOTE_ADDR_MASK** ***IPSEC3_REMOTE_ADDR_MASK** ***IPSEC4_REMOTE_ADDR_MASK** ***IPSEC5_REMOTE_ADDR_MASK**	Query or set the remote subnet mask information (24-bit netmask). AT*IPSEC[VPN number]_REMOTE_ADDR_MASK? to query AT*IPSEC[VPN number]_REMOTE_ADDR_MASK =[subnet mask] to set Default is 255.255.255.0
***IPSEC1_REMOTE_ADDR_TYPE** ***IPSEC2_REMOTE_ADDR_TYPE** ***IPSEC3_REMOTE_ADDR_TYPE** ***IPSEC4_REMOTE_ADDR_TYPE** ***IPSEC5_REMOTE_ADDR_TYPE**	Query or set network information of the IPsec server behind the IPsec gateway for # VPN. AT*IPSEC[VPN number]_REMOTE_ADDR_TYPE? to query AT*IPSEC[VPN number]_REMOTE_ADDR_TYPE=n to set • n=5 — Single Address • n=17 — Subnet Address (default)
***IPSEC1_REMOTE_ID** ***IPSEC2_REMOTE_ID** ***IPSEC3_REMOTE_ID** ***IPSEC4_REMOTE_ID** ***IPSEC5_REMOTE_ID**	Query or set the remote (Peer Identity) ID for the # VPN. • If IP is selected as the remote (Peer Identity) type, AT*IPSEC[VPN number]_REMOTE_ID? returns the WAN IP address assigned by the Mobile Network Operator • If FQDN or User FQDN is selected as the remote (Peer Identity) type, AT*IPSEC[VPN number]_REMOTE_ID? returns the FQDN (for example me@mycompany.com) To set the remote ID: AT*IPSEC[VPN number]_REMOTE _ID=[IP address] or [FQDN], depending on the setting for remote ID (Peer Identity) type.

Table D-6: VPN Commands (Continued)

Command	Description
***IPSEC1_REMOTE_ID_TYPE** ***IPSEC2_REMOTE_ID_TYPE** ***IPSEC3_REMOTE_ID_TYPE** ***IPSEC4_REMOTE_ID_TYPE** ***IPSEC5_REMOTE_ID_TYPE**	Query or set the remote (Peer Identity) ID type for the # VPN. AT*IPSEC[VPN number]_REMOTE_ID_TYPE? to query AT*IPSEC[VPN number]_REMOTE_ID_TYPE=n to set • n=1 — IP • n=2 — FQDN • n=3 — User FQDN *Note:* • *FQDN allows you to use a fully qualified domain name (FQDN) e. g., modemname.domainname.com* • *User FQDN allows you to use a user FQDN whose values should include a username (e.g. user@domain.com)*
***IPSEC1_SHARED_KEY1** ***IPSEC2_SHARED_KEY1** ***IPSEC3_SHARED_KEY1** ***IPSEC4_SHARED_KEY1** ***IPSEC5_SHARED_KEY1**	Query the pre-shared Key (PSK) used to initiate the # VPN tunnel. AT*IPSEC[n]_SHARED_KEY1? [n]=server number
***IPSEC1_STATUS?** ***IPSEC2_STATUS?** ***IPSEC3_STATUS?** ***IPSEC4_STATUS?** ***IPSEC5_STATUS?**	Query the VPN # connection status. AT*IPSEC[VPN number]_STATUS? to query • Disabled • Not Connected • Connected *Note: Use this when troubleshooting a VPN # connection.*
***IPSEC1_TUNNEL_TYPE** ***IPSEC2_TUNNEL_TYPE** ***IPSEC3_TUNNEL_TYPE** ***IPSEC4_TUNNEL_TYPE** ***IPSEC5_TUNNEL_TYPE**	Query or set the VPN # tunnel type. AT*IPSEC[VPN number]_TUNNEL_TYPE? to query AT*IPSEC[VPN number]_TUNNEL_TYPE=n to set • n=0 — Disable the tunnel (default) • n=1 — IPsec Tunnel • n=2 — GRE Tunnel • n=3 — SSL Tunnel *Note: For a successful configuration, all settings for the VPN tunnel must be identical between the AirLink Device VPN and the enterprise VPN server.*

Security

Table D-7: Security AT Commands

Command	Description
F0 (F1, F2, ... F9)	Query or set the Inbound Trusted IP List. ATF? to query the list ATF[n]=d.d.d.d to set • n=0–9 Trusted IP list index number • d.d.d.d = IP Address Using 255 in the IP address will allow any number Example: 166.129.2.255 allows access by all IPs in the range 166.129.2.0–166.129.2.255. Example: atf? 0=192.32.32.21 1=192.32.32.22 2=192.32.32.23 3=0.0.0.0 4=0.0.0.0 5=0.0.0.0 6=0.0.0.0 7=0.0.0.0 8=0.0.0.0 9=0.0.0.0 OK If the index number does not have an IP address associated with it, the query returns 0.0.0.0 for that index number. *Note: You can only query or configure the first nine Inbound Trusted IP addresses with this AT Command. You cannot query or configure Trusted range entries with this AT Command.*
FM	Query or set the Inbound Trusted IP mode (Friends List) — Only allow specified IPs to access the device. ATFM? to query the setting ATFM=n to set • n=0 — Disable Trusted IP mode • n=1 — Enable Trusted IP mode — Only packets from IP addresses in the Trusted IP list are allowed. Packets from other IP addresses are ignored.

Services

Table D-8: Services AT Commands

Command	Description
AirVantage Management System	
***AVMS_ENABLE**	Query or set the AVMS activation status. AT*AVMS_ENABLE? to query AT*AVMS_ENABLE=n to set • n=0—Disable device initiated AVMS management • n=1—Enable device initiated AVMS management
***AVMS_INTERVAL**	Query or set the AVMS communication (heartbeat) interval in seconds. AT*AVMS_INTERVAL? to query AT*AVMS_INTERVAL= n to set • n= INTERVAL (in seconds)
***AVMS_NAME**	Assigns or queries the name to the AirLink device as it appears in AVMS. AT*AVMS_NAME? to query AT*AVMS_NAME= n to set • n= AVMS NAME
***AVMS_SERVER**	Query or set the AVMS server IP address or FQDN. AT*AVMS_SERVER? to query AT*AVMS_SERVER=n to set • n=IP Address or FQDN of AVMS server
***AVMS_STATUS?**	Query the AVMS connection status
Low Power	
***ENGHRS**	Query or set the number of hours the engine has been running. AT*ENGHRS? to query AT*ENGHRS=n to set • n= HOURS Maximum value is 65535.
***POWERMODE?**	Query the current power state/mode. AT*POWERMODE? returns: • Initial—The device is in the initial 5 minutes since power up, so power down event will be ignored • On—Regular power on, a power down is not pending • Low Cancellable—Power down is pending but still Cancellable if the power down trigger goes away • Low Pending 1 and Low Pending 3—Power down is pending, any device tasks are gracefully preparing for the power down • Low Final—Power down is imminent • Low—Power is down

Table D-8: Services AT Commands

Command	Description
PTMR	Query or set the Low Power Mode Delay (in minutes) This is the delay between the time the power down trigger occurs and when the device enters the low power mode. ATPTMR? to query ATPTMR=n to set • n=0–255 (minutes) *Note: There is always a minimum of 1 minute between power down event and actual shutdown (to give the device time to prepare); entering zero will not power down the device immediately.*
VLTG	Query or set the voltage level (threshold for low power mode). When the power drops below this level Low Power Mode is triggered. ATVLTG? to query ATVLTG=n to set • n= 0—Ignore voltage for power control • n= 80–360—threshhold in .1 volt units Example: ATVLTG=130 would place the device in a low power use, standby state if the voltage goes below 13.0V.
Dynamic DNS	
***DOMAIN**	Query or set the domain name used for the IP Manager Dynamic DNS configuration. AT*DOMAIN? to query AT*DOMAIN=DOMAIN to set (up to 20 characters) Example: AT*DOMAIN=eairlink.com **Tip:** *Only letters, numbers, hyphens, and periods can be used in a domain name.* *Note: This AT command is only usable if the Dynamic DNS Service type is set to IP Manager.*

Table D-8: Services AT Commands

Command	Description
***DYNDNS**	Query or set the Dynamic DNS Service type to use. AT*DYNDNS? to query AT*DNYDNS=n to set • n=0—Disable (default) • n=2—dyndns.org • n=5—noip.org • n=6—ods.org • n=8—regfish.com • n=9—tzo.org • n=10—IP Manager *Note: Only IP Manager can be fully configured using AT Commands.*
***IPMANAGER1** ***IPMANAGER2**	*Note: This AT command is only usable if the Dynamic DNS Service type is set to IP Manager.* Query or set a FQDN or IP address of the IP server to send IP change notifications to. You can configure two independent IP Manager servers. AT*IPMANAGER[n]? to query AT*IPMANAGER[n]=SERVER to set. • n=1—First IP Manager server • n=2—Second IP Manager server • SERVER = Server FQDN or IP address Note: You can disable updates to a server by setting blank entry (e.g., “AT*IPMANAGER1=”).
***IPMGRKEY1** ***IPMGRKEY2**	*Note: This AT command is only usable if the Dynamic DNS Service type is set to IP Manager.* Query or set the 128-bit password/key used to authenticate the IP update notifications. If the key's value is all zeros, a default key is used. If all the bytes in the key are set to FF, then no key is used (i.e., the IP change notifications will not be authenticated). AT*IPMGRKEY[n]? to query AT*IPMANAGER[n]=KEY to set • n=1—First IP Manager server • n=2—Second IP Manager server • KEY=128-bit key in hexadecimal [32 hex characters]

Table D-8: Services AT Commands

Command	Description
***IPMGRUPDATE1** ***IPMGRUPDATE2**	*Note: This AT command is only usable if the Dynamic DNS Service type is set to IP Manager.* Query or set the interval (in minutes) to send an IP update notification to the corresponding server. This occurs even if the IP address of the device does not change. If the value is set to 0, then periodic updates are not issued (i.e., IP change notifications is only be sent when the IP actually changes). AT*IPMGRUPDATE[n] to query AT*IPMGRUPDATE[n]=INTERVAL to set • n=0—Disables the update interval (updates only on changes) • n=1—First IP Manager server • n=2—Second IP Manager server • INTERVAL=1–255—interval (in minutes) to send an update
***MODEMNAME**	*Note: This AT command is only usable if AT*DYNDNS is set to 10 (IP Manager).* Query or set the device name used by IP Manager. (This name is displayed on the Status > Home page.) AT*MODEMNAME? to query AT*MODEMNAME=NAME to set (up to 20 characters long) • NAME= device name (for example, mydevice) The value in *DOMAIN provides the domain zone to add to this name. Example: If *MODEMNAME=mydevice and *DOMAIN=eairlink.com, the device's fully qualified domain name is mydevice.eairlink.com. **Tip:** *Each device using IP Manager needs a unique name. I.e., two devices cannot both be called "mydevice". One could be named "mydevice1" while the other could be named "mydevice2".*
SMS	

Table D-8: Services AT Commands

Command	Description

***SMSM2M**
***SMSM2M_8**
***SMSM2M_u**
	You can only use these commands locally.
	• AT*SMSM2M sends an SMS in ASCII text (requires quotation marks; maximum 140 characters)
	• AT*SMSM2M_8 sends an 8-bit SMS (requires quotation marks; maximum 140 characters)
	• AT*SMSM2M_U sends a unicode SMS (requires quotation marks; maximum 140 characters)
	Format:
	AT*SMSM2M=“[phone] [ascii message]”
	AT*SMSM2M_8=“[phone] [hex message]”
	AT*SMSM2M_U=“[phone] [hex message]”
	• The phone number can only consist of numbers (NO spaces or other characters). The phone number should be as it appears in the Last Incoming Phone Number field.
	  • Example 1 (US): 14085551212 (including leading 1 and area code)
	  • Example 2 (US): 4085551212 (ignore leading 1, include area code)
	  • Example 3 (UK): 447786111717 (remove leading 0 and add country code)
	Command Examples:
	AT*SMSM2M=”18005551212 THIS IS A TEST” sends in ASCII.
	AT*SMSM2M_8="17604053757 5448495320495320412054455354" sends the message “THIS IS A TEST” as 8-bit data.
	AT*SMSM2M_U="17604053757 000102030405060708090a0b0c0d0e0f808182838485868788898A8b8c8d8e8f" sends the bytes:
	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
	80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f
	Note: Not all cellular Mobile Network Operators support 8-bit or unicode SMS messages.

***SMS_PASSWORD**	Query or set the SMS password. AT*SMS_PASSWORD? to query AT*SMS_PASSWORD = n n= SMS password If no password has ever been configured, a default password is created from the last four characters of the SIM ID (for all SIM-based devices) or the ESN (for devices without a SIM, such those using EV-DO). *Note: The configured password remains in place, even when the device is reset to factory default settings.*

Table D-8: Services AT Commands

Command	Description
***SMSWUPTOUT**	This AT Command only to OpenSIM devices on the Vodafone network. Query or set the connection timeout for the SMS Wakeup feature. When this feature is enabled, an IP connection is initiated on receipt of a specific type of SMS (For information on choosing the type of SMS, see Services > SMS >SMS Wakeup > SMS Wakeup Trigger described in step 3 on page 210). The IP connection closes after the timeout period specified in this AT command. Outgoing traffic sent after the timer is set does not reset the timer. AT*SMSWUPTOUT? to query AT*SMSWUPTOUT=n to set • n=2–65535 minutes (default is 2) See also *RADIO_CONNECT on page 400.
Telnet/SSH	
***DEFAULTTELNETUSER**	Query or set the Telnet default user name AT*DEFAULTTELNETUSER? to query AT*DEFAULTTELNETUSER=n to set • n=None—Prompted for a user name and password when logging into a Telnet session (default) • n=user—Prompted for a password only when logging into a Telnet session (User name is “user”.) *Note: The default user name is only for Telnet; not SSH.*
***TELNETTIMEOUT**	Query or set the Telnet/SSH idle time out. By default, this value is set to close the telnet/SSH connection if no data is received for 2 minutes. AT*TELNETTIMEOUT? to query AT*TELNETTIMEOUT=n to set • n=1—255 minutes (Default is 2.)
***TSSH**	Query or set the remote login server mode. AT*TSSH? to query AT*TSSH=n to set • n=0—Telnet (default) • n=1—SSH
***TPORT**	Query or set the Telnet/SSH port. AT*PORT? to query AT*PORT=n to set • n=1–65535 (Default is 2332.) Many networks have the ports below 1024 blocked. It is recommended to use a higher numbered port.
***TQUIT**	AT*TQUIT which will kill an open telnet session to the LS300 or GX4x0 device.
Management (SNMP)	
SNMP General Configuration	

Table D-8: Services AT Commands

Command	Description
***SNMP**	Query or set the SNMP option. AT*SNMP? to query AT*SNMP=n to set • n=0—Disable • n=1—Enable
***SNMPCONTACT**	Add string contact information in SNMPv2 and SNMPv3. AT*SNMPCONTACT=string • string= email address (Example: admin@sierrawireless.com)
***SNMPLOCATION**	Add string location information in SNMPv2 and SNMPv3. AT*SNMPLOCATION=string • string= location information (Example: Building 19–67B)
***SNMPNAME**	Add string name in SNMPv2 and SNMPv3. AT*SNMPNAME=STRING • STRING=name (Example: John Doe)
***SNMPPORT**	Query or set the port number in SNMPv2 and SNMPv3. AT*SNMPPORT? to query AT*SNMPPORT=n to set • n=1–65535 (Default is 161.)
***SNMPVERSION**	Query or set the SNMP version. AT*SNMPVERSION? to query AT*SNMPVERSION=n to set • n=2—version 2 • n=3—version 3
SNMP Read Only Configuration	
***SNMPPROCOMMUNITY**	Read-only community string in SNMPv2 and SNMPv3 (SNMP equivalent of a password; for example: public)
***SNMPROUSER**	Query or set a read only SNMP username string in SNMPv3.
***SNMPROUSERAUTHTYPE**	Query or set the read only authentication type in SNMPv3. AT*SNMPROUSERAUTHTYPE? to query AT*SNMPROUSERAUTHTYPE=n • n=0—MD5 • n=1—SHA
***SNMPROUSERSECLVL**	Query or set the read only security level in SNMPv3. AT*SNMPROUSERSECLVL? to query AT*SNMPROUSERSECLVL=n to set • n=0—none • n=1—authentication only • n=2—authentication + privacy
SNMP Read/Write Configuration	

Table D-8: Services AT Commands

Command	Description
***SNMPRWCOMMUNITY**	Read/write community string in SNMPv2 and SNMPv3. (SNMP equivalent of a password; for example: private)
***SNMPRWUSER**	Query or set a read/write SNMP username string in SNMPv2 and SNMPv3.
***SNMPRWUSERAUTHTYPE**	Query or set the read/write authentication type in SNMPv3. AT*SNMPRWUSERAUTHTYPE? to query AT*SNMPRWUSERAUTHTYPE=n to set • n=0—MD5 • n=1—SHA
***SNMPRWUSERSECLVL**	Query or set the read/write security level in SNMPv3. AT*SNMPRWUSERSECLVL? to query AT*SNMPRWUSERSECLVL=n to set • n=0—none • n=1—authentication only • n=2—authentication + privacy
***SNMPRWUSERPRIVTYPE**	Query or set the read/write privacy type in SNMPv3. AT*SNMPRWUSERPRIVTYPE? to query AT*SNMPRWUSERPRIVTYPE=n to set • n=0—DES • n=1—AES
SNMP TRAP Configuration	
***SNMPENGINEID**	Specify an identification name string for a SNMP engine in SNMPv3. (For example: Shark-0012E8)
***SNMPTRAPAUTHTYPE**	Query or set the SNMP TRAP authentication type in SNMPv3. AT*SNMPTRAPAUTHTYPE? to query AT*SNMPTRAPAUTHTYPE=n to set • n=0—MD5 • n=1—SHA
***SNMPTRAPCOMMUNITY**	SNMP TRAP community string in SNMPv2 and SNMPv3. (SNMP equivalent of a password)
***SNMPTRAPDEST**	Query or set the SNMP TRAP destination in SNMPv2 and SNMPv3. (for example: 192.168.13.33)
***SNMPTRAPPORT**	• Query or set the SNMP TRAP port in SNMPv2 and SNMPv3. 1–65535 (Default is 162.)
***SNMPTRAPPRIVTYPE**	Query or set the SNMP TRAP privacy type in SNMPv3. AT*SNMPTRAPPRIVTYPE? to query AT*SNMPTRAPPRIVTYPE=n to set • n=0—DES • n=1—AES

Table D-8: Services AT Commands

Command	Description
***SNMPTRAPSECLVL**	Query or set the SNMP TRAP security level in SNMPv3. AT*SNMPTRAPSECLVL? to query AT*SNMPTRAPSECLVL=n to set • n=0—none • n=1—authentication only • n=2—authentication + privacy
***SNMPTRAPUSER**	Query or set a SNMP TRAP username string in SNMPv3.
Email (SMTP) Commands	
***SMTPADDR**	Query or set the mail server IP address or FQDN. AT*SMTPADDR? to query AT*SMTPADDR=[d.d.d.d] or [NAME] to set • d.d.d.d=IP Address • NAME=domain name (maximum: 40 characters)
***SMTPFROM**	Query or set the email address from which the SMTP message is being sent (required by some mail servers). AT*SMTPFROM? to query AT*SMTPFROM=EMAIL to set • EMAIL=email address (maximum: 30 characters)
***SMTPSUBJ**	Query or set the email subject line to use for sending emails. AT*SMTPSUBJ? to query AT*SMTPSUBJ=STRING to set
***SMTPPW**	Query or set the email server password (required by some mail servers). AT*SMTPPW? to query AT*SMTPPW=PASSWORD to set
***SMTPUSER**	Query or set the email account username (required by some mail servers). AT*SMTPUSER? to query AT*SMTPUSER=USER to set (maximum: 40 characters)
Time (SNTP) Commands	
***SNTP**	Query or set daily SNTP updates of the system time. AT*SNTP? to query AT*SNTP=n to set • n=0—Off • n=1—On
***SNTPADDR**	SNTP Server IP address, or fully-qualified domain name, to use if *SNTP=1. AT*SNTPADDR? to query AT*SNTPADDR=[d.d.d.d] or [NAME] • d.d.d.d=IP Address • NAME=FQDN

GPS

Table D-9: GPS AT Commands

Command	Description
***GPSDATA?**	Query the device and provides a snap-shot of GPS data. This command is independent of all GPS configuration. You don't need to have a server configured or any specific report type selected. The response to this command lists the fix status, satellite count, and latitude and longitude in decimal degrees. It is not formatted as a GPS report. For example: AT*GPSDATA? returns: GPS Fix=1 Satellite Count=8 Latitude=+49.17081 Longitude=-123.06970
***PGPS**	Query or set the serial streaming interface ports that the reports are sent to. AT*PGPS? to query AT*PGPS=n to set • n=0—None • n=1—DB9 Serial • n=2—USB Serial • n=3—DB9 and USB • n=4—I/O X-Card Serial • n=5—I/O X-Card Serial and DB9 • n=6—I/O X-Card Serial and USB • n=7—I/O X-Card Serial, DB9 and USB
***PGPSC**	Query or set the out-of-coverage setting. This setting enables you to configure the AirLink device to stream GPS reports to the serial port only when the device has no cellular coverage. (This enables you to use a back-up in-vehicle mapping application that does not rely on cellular network coverage. AT*PGPSC? to query AT*PGPSC=n to set • n=0: ALWAYS (default) GPS reports are always streamed to the serial port • n=1: Out of Coverage—GPS reports are only streamed to the serial port when the AirLink device has no cellular network connection. *Note: The two persistent GPS report parameters, *PGPSR and *PGPSF, control the report type and message frequency of reports sent out the serial port when the AirLink device is out of cellular network coverage.*

Table D-9: GPS AT Commands (Continued)

Command	Description
***PGPSD**	Query or set the delay (in seconds) before the out-of-coverage stream begins sending the messages out the serial port and not into SnF. AT*PGPSD? to query AT*PGPSD=n to set • n=0 (default) • n=1–255 *Note: Any messages put into SnF during this switch-over delay period are sent over the air when coverage is re-acquired.* *Note: The two persistent GPS report parameters, *PGPSR and *PGPSF, control the report type and message frequency of reports sent out the serial port when the AirLink device is out of cellular network coverage.*
***PGPSF**	Query or set how frequently (in seconds) the GPS report is sent to the serial link. AT*PGPSF? to query AT*PGPSF=n to set • n= 0–65535
***PGPSR**	Query or set the GPS report type. AT*PGPSR? to query AT*PGPSR=n to set NMEA reports: • n=E0—NMEA GGA + VTG • n=E1—NMEA GGA+VTG+RMC • n=E2—NMEA GGA+VTG+RMC+GSA+GSV TAIP reports: • n=F0—TAIP data • n=F1—TAIP compact data • n=F2—TAIP LN report • n=F3—TAIP TM report
***PPDIST** ***PP2DIST** ***PP3DIST** ***PP4DIST**	Query or set the GPS report distance interval in 100 meter units. For example, if you entered a value of 635, it would translate to 63,500 meters (63.5 kilometers). AT*PP[Server number if other than server 1]DIST? to query AT*PP[Server number if other than server 1]DIST=n to set • n=0 — Disabled • n=1–65535 — Distance in 100 meter units that the device moves before sending a GPS report

Table D-9: GPS AT Commands (Continued)

Command	Description
***PPDISTM** ***PP2DISTM** ***PP3DISTM** ***PP4DISTM**	Query or set the GPS report distance Interval in meters. AT*PP[Server number if other than server 1]DISTM? to query AT*PP[Server number if other than server 1]DISTM=n to set • n=0 — Disabled • n=40–65535—Distance in meters that the device moves before sending a GPS report *Note: If you enter a value greater than zero, but less than 40, ALEOS rounds it up to 40.*
***PPDEVID**	Query or set whether or not the RAP GPS report includes device ID and if so, which type of device ID is included. AT*PPDEVID? to query AT*PPDEVID=n to set • n=0—None • n=1—Phone number • n=2—ESN/IMEI *Note: The device ID in the RAP report is in hex, not plain text.*
***PPFLUSHONEVT**	Query or set Send SnF Buffer Immediately on input. If this feature is enabled, any pending stored reports are sent if the I/O input changes, a stationary vehicle is moved, or a maximum speed is exceeded. AT*PPFLUSHONEVT? to query AT*PPFLUSHONEVT=n to set • n=0—Disable • n=1—Enable

Table D-9: GPS AT Commands (Continued)

Command	Description
***PPGPSR** ***PP2GPSR** ***PP3GPSR** ***PP4GPSR**	Query or set the GPS report type. AT*PP[Server number if other than server 1]GPSR? to query AT*PP[Server number if other than server 1]GPSR=n to set RAP reports: • n=0 — Use legacy reports specified in *MF value. Note: Must also have *PPDEVID=0. • n=11 — Standard GPS Report • n=12 — Standard GPS Report + UTC Date • n=13 — Standard GPS Report + UTC Date + RF data • n=14—Standard GPS report + GPS + Date + RF + EIO Xora reports • n=D0 — Xora NMEA reports • n=E0 — GGA and VTG NMEA reports • n=E1 — GGA, VTG and RMC NMEA reports • n=E2 — GGA, VTG, RMC, GSA and GSV NMEA reports TAIP reports • n=F0 —TAIP data—TAIP GPS report that contains position and velocity • n=F1 —TAIP GPS report that contains the compact position • n=F2—TAIP LN report—TAIP GPS report that contains a long navigation message • n=F3—TAIP TM report—TAIP GPS report that contains the time and date
***PPINPUTEVT** ***PP2INPUTEVT** ***PP3INPUTEVT** ***PP4INPUTEVT**	Query or set ability to send a special report for digital input changes. AT*PP[Server number if other than server 1]INPUTEVT? to query AT*PP[Server number if other than server 1]INPUTEVT=n to set • n=0 — Disable • n=1 — Enable
***PPIP** ***PP2IP** ***PP3IP** ***PP4IP**	Query or set the IP address where GPS reports are sent. See also *PPPORT on page 427. AT*PP[Server number if other than server 1]IP? to query AT*PP[Server number if other than server 1]IP=d.d.d.d to set • d.d.d.d=IP address Example: AT*PPIP=192.100.100.100
***PPLATS**	Query or set the local reporting interval (in seconds). AT*PPLATS? to query AT*PPLATS=n to set • n=0—Disable (default) • n=1–255 (seconds)

Table D-9: GPS AT Commands (Continued)

Command	Description
***PPLATSEXTRA**	Query or set the number of additional consecutive ports that the local GPS report is sent to. AT*PPLATSEXTRA? to query AT*PPLATSEXTRA=n to set • n=0—Just the original report is sent (default). • n=1–7—Send GPS report copies to that number of ports. Example: If AT*PPLATSEXTRA=7 and the port in S53 is 1000, then GPS reports will be sent to ports 1000–1008.
***PPLATSR**	Query or set the GPS report type that is sent to the local client (Ethernet, USB/net, or PPP). AT*PPLATSR? to query AT*PPLATSR=n to set RAP reports: • n=11—GPS Data • n=12—GPS + Date • n=13—GPS + UTC + RF • n=14—GPS + Date + RF + EIO NMEA reports: • n=E0—NMEA GGA + VTG • n=E1—NMEA GGA + VTG + RMC • n=E2—NMEA GGA + VTG + RMC + GSA + GSV TAIP reports: • n=F0 —TAIP data—TAIP GPS report that contains position and velocity • n=F1 —TAIP GPS report that contains the compact position • n=F2—TAIP LN report—TAIP GPS report that contains a long navigation message • n=F3—TAIP TM report—TAIP GPS report that contains the time and date
***PPMAXRETRIES** ***PP2MAXRETRIES** ***PP3MAXRETRIES** ***PP4MAXRETRIES**	Query or set maximum number retries when in Simple Reliable mode, UDP Sequence mode, and TCP transports. AT*PP[Server number if other than server 1]MAXRETRIES? to query AT*PP[Server number if other than server 1]MAXRETRIES=n to set • n=0—Disabled • n=1–255 retries (Maximum is 10.)
***PPMINTIME** ***PP2MINTIME** ***PP3MINTIME** ***PP4MINTIME**	Query or set the minimum amount of time between report packets. Each packet can contain multiple reports. This is useful to limit network traffic and make more efficient use of bandwidth. You can also use it in conjunction with store and forward. The minimum value depends on the policies of the Mobile Network Operator. AT*PP[Server number if other than server 1]MINTIME? to query AT*PP[Server number if other than server 1]MINTIME=n to set • n=0—Disable • n=1–65535 seconds

Table D-9: GPS AT Commands (Continued)

Command	Description
***PPODOM** ***PP2ODOM** ***PP3ODOM** ***PP4ODOM**	Query or set including the current odometer reading in the RAP report. AT*PP[Server number if other than server 1]ODOM? to query AT*PP[Server number if other than server 1]ODOM=n to set • n=0—Disabled (default) Do not include odometer reading in report. • n=1—Enabled Include odometer reading in report.
***PPODOMVAL**	Query or set the odometer value (in meters). Maximum value is approximately 4.3 billion meters (2.7 million miles). AT*PPODOMVAL? to query AT*PPODOMVAL=n to set • n=0–4294967295 meters
***PPPORT** ***PP2PORT** ***PP3PORT** ***PP4PORT**	Query or set the port GPS reports are sent to. AT*PP[Server number if other than server 1]PORT? to query AT*PP[Server number if other than server 1]PORT=n to set • n=0—Disable • n=1–65535
***PPREPORTINPUTS** ***PP2REPORTINPUTS** ***PP3REPORTINPUTS** ***PP4REPORTINPUTS**	Query or set input reporting and including the current digital input value in RAP reports. AT*PP[Server number if other than server 1]REPORTINPUTS? to query AT*PP[Server number if other than server 1]REPORTINPUTS=n to set • n=0—Disabled • n=1—Enabled
***PPSIMPLETO** ***PP2SIMPLETO** ***PP3SIMPLETO** ***PP4SIMPLETO**	Query or set the first retry interval for Simple Reliable, UDP Sequence mode, and TCP transports (in seconds). AT*PP[Server number if other than server 1]SIMPLETO? to query AT*PP[Server number if other than server 1]SIMPLETO=n to set • n=0—Disable • n=1–255 (Default is 10.)
***PPSNF** ***PP2SNF** ***PP3SNF** ***PP4SNF**	Query or set the Store and Forward (SNF) setting. SNF causes GPS reports to be stored if the device/vehicle goes outside the area of network coverage. Once the vehicle is in the coverage area, the GPS reports are sent en masse to the server. AT*PP[Server number if other than server 1]SNF? to query AT*PP[Server number if other than server 1]SNF=n to set • n=0—Disabled • n=1—Enabled (default)
***PPSNFR** ***PP2SNFR** ***PP3SNFR** ***PP4SNFR**	Query or set Transport / SNF mode. GPS reports are retransmitted if not acknowledged by the server. AT*PP[Server number if other than server 1]SNFR? to query AT*PP[Server number if other than server 1]SNFR=n to set • n=0—Disabled • n=1—Reliable mode • n=2—Simple Reliable mode • n=3—UDP Sequence • n=4—TCP Listen • n=5—TCP

Table D-9: GPS AT Commands (Continued)

Command	Description
***PPTAIPID**	Query or set the four character alphanumeric TAIP ID. AT*PPTAIPID? to query AT*PPTAIPID=nnnn to set • nnnn=alphnumeric characters
***PPTIME** ***PP2TIME** ***PP3TIME** ***PP4TIME**	Query or set the GPS report time interval (in seconds). AT*PP[Server number if other than server 1]TIME? to query AT*PP[Server number if other than server 1]TIME=n to set • n=0 – 65535 seconds *Note: Your cellular Mobile Network Operator may impose a minimum transmit time.* See also *PPMINTIME, *PPTSV, +CTA. *Note: A report time of less than 30 seconds may keep an RF link up continuously, tying up an RF resource to transfer small amounts of data. Generally, the RF channel is released and goes dormant in 10–20 seconds if no data is sent or received.*
***PPTCPPOLL**	Query or set the port to listen on for TCP GPS report polling. *Note: The request to this port needs to come from the same IP address in *PPIP on page 425 and uses the report type configured for server 1.* AT*PPTCPPOLL? to query AT*PPTCPPOLL=n to set • n=0—Disabled • n=1–65535 (default 9494)
***PPTSV** ***PP2TSV** ***PP3TSV** ***PP4TSV**	Query or set the time interval in minutes that the device sends in reports when it is stationary (Stationary vehicle timer). AT*PP[Server number if other than server 1]TSV? to query AT*PP[Server number if other than server 1]TSV=n to set • n=0—Disabled • n=1–255 minutes For example, if *PPTIME=10, the device sends GPS reports at least once every 10 seconds while it is moving; however, once it stops moving, it slows the reports down to this *PPTSV value. *Note: In order for the PPTSV (Stationary Vehicle timer) to take effect, the PPTIME value must be set to a value greater than 0 and less than the PPTSV value. The PPTSV timer checks for vehicle movement at the PPTIME interval, so if PPTIME is disabled, then PPTSV will also be disabled.*

Serial

Table D-10: Serial AT Commands

Command	Description
AIP	Query or set the option to allow IP addresses to communicate on UDP over serial. AT*AIP? to query AT*AIP=n to set • n=0 — Allow only the IP address specified in S53 to connect when UDP auto answer is enabled (S82=2) • n=1 — Allow any incoming IP address to connect when UDP auto answer is enabled (S82=2) Always subject to any security filters that may be defined. (See Security on page 412.)
\APPP	Initiates a PPP connection on serial terminal. You can only use \APPP locally. You can also initiate a PPP connection using the ADT command and one of the supported phone numbers. *Note: PPP is not available on the I/O X-Card serial port.*
***CTSE**	Query or set asserting Clear To Send (CTS) when there is a network coverage. AT*CTSE? to query AT*CTSE=n to set • n=0 — Disabled (default) • n=1 — Enable assertion of CTS when there is network coverage
DAE	Query or set AT Escape Sequence detection. ATDAE? to query ATDAE=n to set • n=0 — Enable • n=1 — Disable (The escape sequence (+++) is ignored.)
***DPORT**	Query or set the device port that the device listens on for inbound packets/data/polls. AT*DPORT? to query AT*DPORT=n to set • n=1–65535
***DU**	Query or set the dial command to only use UDP. AT*DU? to query AT*DU=n to set • n=0 — Dial using the means specified (default) • n=1 — Dial UDP always, even when using ATDT When this parameter is set you cannot establish a TCP PAD connection by using the Dial command.

Table D-10: Serial AT Commands (Continued)

Command	Description
***ENQ**	Query or set the option to output an ENQ [0x05] after the TCP CONNECT, delayed by the Delay Connect Response time (S221). AT*ENQ? to query AT*ENQ=n to set • n=0 — Disable (default) • n=1 — Enable ENQ on TCP CONNECT
***HOSTMODE?**	Query the current host mode. AT*HOSTMODE? returns: • AT • PPP • TCP • UDP *Note: If the device is not in AT mode, Telnet into the device to execute this command.*
MD	Query or set the default start-up mode for the serial port. When the device is power-cycled, the serial port enters the mode specified by this command after 5 seconds. On startup, typing ATMD0 within 5 seconds changes the mode to normal (AT command) mode. See also S53 to set the port for UDP. AT*MD? to query AT*MD=hh to set • hh (hex byte)=00 — Normal (AT Command mode) • hh=02 — PPP • hh=03 — UDP • hh=04 — TCP • hh=08 — reverse telnet/ssh • hh=13 — Modbus ASCII • hh=23 — Modbus RTU (Binary) • hh=33 — BSAP • hh=63 — Variable Modbus • hh=83 — UDP Multiple Unicast *Note: The I/O X-Card only supports AT, UDP, and TCP.*

Table D-10: Serial AT Commands (Continued)

Command	Description
MLIST	Add IP addresses to the Modbus address list or query the Modbus address list, using decimal index values. Format is MLISTIndex(decimal)=IP address Example: ATMLIST10=123.123.123.123, where: • 10 is the Index • 123.123.123.123 is the IP address MLISTIndex=IP to add an IP address to the list Including the port number after the IP address is optional. If you include the port number, separate the port number and IP address by a colon. For example: 10=123.123.123.123:11223 MLIST? to query the Modbus address list; returns the addresses in the list in the format Index=IP. For example: 10=123.123.123.123 11=124.124.124.124 12=125.125.125.125 13=126.126.126.126 Range for index numbers is 0—65535. The Modbus address list accepts up to 100 entries. *Note: This command is not supported on the I/O X-Card serial port.*
MLISTX	Add IP addresses to the Modbus address list or query the Modbus address list, using hexadecimal index values. Format is MLISTXIndex(hex)=IP address Example: ATMLISTX000A=123.123.123.123, where: • 000A is the Index • 123.123.123.123 is the IP address MLISTXIndex=IP to add an IP address to the list Including the port number after the IP address is optional. If you include the port number, separate the port number and IP address by a colon. For example: 0xA=123.123.123.123:11223 MLISTX? to query the Modbus address list returns; returns the addresses in the list in the format Index=IP. For example: 000A=123.123.123.123 000B=124.124.124.124 000C=125.125.125.125 000D=126.126.126.126 Range for index numbers is 0—FFFF. The Modbus address list accepts up to 100 entries. *Note: This command is not supported on the I/O X-Card serial port.*

Table D-10: Serial AT Commands (Continued)

Command	Description
MVLEN	Query or set the length of the Modbus Variant ID. ATMVLEN? to query ATMVLEN=[length of the RTU ID in bytes] to set *Note: This command is not supported on the I/O X-Card serial port.*
MVMSK	Query or set the Modbus Variant ID Mask (byte hex mask to use when extracting the ID). This parameter is used when the when the Mode Default (MD on page 430) is set to hex 63. ATMVMSK? to query ATMVMSK=[byte hex mask] to set *Note: This command is not supported on the I/O X-Card serial port.*
MVOFF	Query or set the Modbus (Variable mode) offset in the data where the Modbus ID starts. ATMVOFF? to query ATMOFF=n to set • n= 0–255 *Note: This command is not supported on the I/O X-Card serial port.*
MVTYP	Query or set the Modbus Variant type (RTU ID data-type in a modbus-variant protocol). This parameter is used when MD on page 430 is set to 63. It defines the data-type of the RTU ID in Modbus-like protocol data packets. ATMVTYP? to query ATMVTYP=n to set • n=0—Binary • n=1—ASCII hex • n=2—ASCII decimal *Note: This command is not supported on the I/O X-Card serial port.*
IPL	Query or set the IP list dial. AT*IPL? to query AT*IPL=n to set • n=0—Disable • n=1—Enable This allows you to access to the Modbus IP address list using the first two digits of the dial string. Example: ATDT1234567 would go to ID “12” on the Modbus list and use the associated IP as the destination.

Table D-10: Serial AT Commands (Continued)

Command	Description
***NUMTOIP**	Query or set the option to convert a 12-digit number to an IP address For example, converts 111222333444 to 111.222.333.444 AT*NUMTOIP? to query AT*NUMTOIP=n to set • n=0—Disable • n=1—Enable
S50	Query or set the data forwarding idle time-out. ATS50? to query ATS50=n to set • n=0 — a forwarding time-out of 10ms is used. • n= tenths of a second
S51	Query or set the PAD data forwarding character. ASCII code of character that causes data to be forwarded. Used in UDP or TCP PAD mode. ATS51? to query AT51=CHARACTER to set • n=0 — No forwarding character • n= CHARACTER
S53	Query or set the method (dial mode), destination IP address, and port used as defaults for the D (Dial) AT command. ATS53? to query ATS53=[method][d.d.d.d][/ppppp] to set [method] can be: • P — UDP • T — TCP [d.d.d.d] is the destination IP address [pppp] is the port number. Example: ATS53=P111.22.33.44/5555 where: • The first character is the dial mode (P in this example) • Followed by destination IP address (111.22.33.44 in this example) • A slash • Followed by the destination port (5555 in this example) You can also use this command to set only the port. For example, AT53=/7777.
S60	Query or set the Telnet Client Echo Mode. ATS60? to query ATS60=n to set • n=0 — No Echo • n=1 — Local Echo (default) • n=2 — Remote Echo

Table D-10: Serial AT Commands (Continued)

Command	Description
S82	Query or set UDP auto answer. ATS82? to query ATS82=n to set • n=0 — Disable • n=1 — Enable
S83	Query or set the UDP auto answer idle time-out. If no data is sent or received before the time-out occurs, the current UDP session is terminated. While a session is active, packets from other IP addresses are discarded (unless *UALL is set). ATS83? to query ATS83=n to set • n=0 — No idle time-out (default) • n=1 – 255 — Time-out in seconds
***SERIALLEDDISPLAY**	Query or set whether or not the Activity LED on the AirLink device indicates traffic on the selected serial port. AT*SERIALLEDDISPLAY? to query AT*SERIALLEDDISPLAY=n to set • n=0 — LED display of serial traffic disabled (default) • n=1 — LED display of serial traffic enabled For a description of the Activity LED when this parameter is enabled, see Display on page 302.
***SERIALLEDPORT**	Query or set the serial port that the Activity LED indicates traffic on if AT*SERIALLEDDISPLAY is set to 1. AT*SERIALLEDPORT? to query AT*SERIALLEDPORT=n to set • n=0 — Main serial port on the AirLink device itself (default) • n=1 — Serial port on the I/O X-Card (applies only to an AirLink GX Series device with an I/O X-Card installed)
TCPS	Query or set the TCP connection time-out (TCPS) units. If there is no traffic through the TCP connection for the specified interval, the connection is terminated. AT*TCPS? to query AT*TCPS=n to set • n=0 — minutes • n=1—seconds
TCPT	Query or set the interval to terminate a TCP connection when there is no traffic. This value affects only the TCP connection in TCP PAD mode. AT*TCPT? to query AT*TCPT=n to set • n=0–255
***UALL**	Query or set the ability to accept UDP packets from any IP address when a UDP session is active. If there is no UDP session active, an incoming UDP packet will be treated according to the UDP auto answer and AIP settings. AT*UALL? to query AT*UALL=n to set • n=0 — No effect (default) • n=1 — Accept UDP data from all IP addresses when in a UDP session

Table D-10: Serial AT Commands (Continued)

Command	Description
***UDPLAST**	Query or set the option to set S53 to the last accepted IP address through UDP auto answer. This can be used in conjunction with MD3 so that when there is no UDP session, new Ethernet host data will cause a connection to be restored to the last IP accepted through UDP auto answer. AT*UDPLAST? to query AT*UDPLAST=n to set • n=0 — Does not change destination IP (default) • n=1 — Change destination IP to last received
***USD**	Query or set the specified delay before sending the UDP packets out the serial port. AT*USD? to query AT*USD=n to set • n=0 — No UDP packet delay (default) • n=1 – 255 — Delay in 100ms units, from 100 ms to 25.5 sec.

Standard (Hayes) commands

The following table contains Hayes commands supported on AirLink devices.

Table D-11: Standard (Hayes) AT Commands

Command	Description
+++	AT escape sequence (not preceded by AT) If a serial terminal is in a data mode, typing this sequence on that serial terminal causes the terminal to re-enter AT command mode. There must be an idle time on the serial port before and after the sequence. The idle time is set by the value in S50. After you type the AT escape sequence, the terminal remains in AT command mode for 15 seconds before it automatically leaves AT command mode and returns to the previous data mode. *Note: The "+" is ASCII character 0x2B.* *Note: The detection of this sequence is disabled if DAE=1.*
&C	Query or set Data Carrier Detect (DCD) mode. DCD is a hardware signal that notifies the software that the device is communicating with another device. AT&C? to query AT&Cn to set • n=0 — Always assert DCD • n=1 — Assert DCD enable when network is ready (default) If you have a GX Series device with an I/O X-Card installed, you can query or set the main port on the device or the port on the X-Card by specifying the port number. If no port is specified, the query or command affects the port your are telnetting to. AT&C?,[p] to query AT&Cn,[p] to set • p=0—Main serial port on the device • p=1—Serial port on the I/O X-Card *Note: Do not use an equal sign (=) when issuing the command.*

Table D-11: Standard (Hayes) AT Commands (Continued)

Command	Description
D[*method*] [*d.d.d.d*] [*/ppppp*] or D[*method*] [[@]*name*] [*/ppppp*]	Dial a connection to a remote IP and Port using either UDP, TCP, or Telnet. You can only use ATD#19788 and ATDT#19788 locally. *method* = P — Establish a UDP connection T — Establish a TCP connection N — Establish a Telnet connection *d.d.d.d* = IP address to establish connection to *name* = Domain name to establish connection to *ppppp* = IP port to establish connection to Examples: **ATD** — Dial (establish) default connection per **S53** **ATDP***nnn.nnn.nnn.nnn*[/ppppp] — Dial (establish) UDP session to the specified IP address/port. If the method, IP address, or port is omitted, the values from S53 are used. If a Telnet connection is requested (N) and the port is not supplied, port 23 will be used instead of the value from S53. Several special dialing numbers exist to make it easy to establish a **PPP** connection with the device. **ATD#19788** or **ATDT#19788** will establish a PPP connection (see \APPP on page 429). If a domain name is specified, the '@' symbol can be used to explicitly indicate the start of the name. For example, if "**ATDPHONY**" is issued, this will be interpreted as dial a UDP connection to "HONY". To dial using the default method to host "PHONY", one would issue "ATD@PHONY". To end the connection, issue the **+++** escape sequence or drop the DTR line (if Ignore DTR **S211=0** or **&D2**). *Note: The source port of the session is the **Device Port** (set by ***DPORT**).*
&D	Query or set Data Terminal Ready (DTR) mode. AT&D? to query AT&Dn to set • n=0 — Devices ignores DTR, same effect as HW DTR always asserted (same as S211=1); DTD is assumed to be on. • n=1 — DRT drop causes the device to switch to AT command mode, but does not drop the connection. • n=2 — DTR drop causes the connection to drop. • n=3—DTR drop causes the connection to reinitialize. If you have a GX Series device with an I/O X-Card installed, you can query or set the main port on the device or the port on the X-Card by specifying the port number. If no port is specified, the query or command affects the port your are telnetting to. AT&D?,[p] to query AT&Dn,[p] to set • p=0—Main serial port on the device • p=1—Serial port on the I/O X-Card *Note: Do not use an equal sign (=) when issuing the command.*

Table D-11: Standard (Hayes) AT Commands (Continued)

Command	Description
***DATZ**	Query or set the option to block device reset using ATZ. AT*DATZ? to query AT*DATZ=n to set • n=0 — Off. Block is disabled—ATZ resets the device. (default) • n=1 — On. Block is enabled—ATZ does not reset the device.
E	Toggle AT command echo mode. ATE? to query ATEn to set • n=0 — Echo Off; does not echo commands to the computer • n=1 — Echo On; echoes commands to the computer (so you can see what you type) *Note: Do not use an equal sign (=) when issuing the command.*
H	ATH hangs up, immediately terminates the session (PAD or PPP).
HOR	Half-Open Response — In UDP auto answer (half-open) mode. AT*HOR? to query AT*HOR=n to set • n=0 — No response codes when UDP session is initiated • n=1 — RING CONNECT response codes sent out serial link before the data from the first UDP packet *Note: Quiet Mode must be Off.*
Q	Query or set AT quiet-mode. If quiet mode is set, there is no responses to AT commands except for data queried. ATQ? to query ATQn to set • n=0 — Off (default) • n=1 — Quiet-mode on *Note: Do not use an equal sign (=) when issuing the command.*

Table D-11: Standard (Hayes) AT Commands (Continued)

Command	Description
\Q	Query or set the serial port flow control. AT\Q? to query AT\Qn to set • n=0 — No flow control • n=1 — Hardware flow control • n=4 — Transparent software flow control If you have a GX Series device with an I/O X-Card installed, you can query or set the main port on the device or the port on the X-Card by specifying the port number. If no port is specified, the query or command affects the port your are telnetting to. AT\Q?,[p] to query AT\Qn,[p] to set • p=0—Main serial port on the device • p=1—Serial port on the I/O X-Card *Note: Do not use an equal sign (=) when issuing the command.*
&S	Query or set DSR. AT&S? to query AT&Sn to set • n=0—Always assert • n=1—Assert DSR while in data mode (UDP, TCP, PPP) If you have a GX Series device with an I/O X-Card installed, you can query or set the main port on the device or the port on the X-Card by specifying the port number. If no port is specified, the query or command affects the port your are telnetting to. AT&S?,[p] to query AT&Sn,[p] to set • p=0—Main serial port on the device • p=1—Serial port on the I/O X-Card *Note: Do not use an equal sign (=) when issuing the command.*
S0	Query or set TCP auto answer (the number of rings required before the device automatically answers a call). ATS0? to query ATS0n to set • n=0— Disable • n=1—Enable *Note: Do not use an equal sign (=) when issuing the command.*

Table D-11: Standard (Hayes) AT Commands (Continued)

Command	Description
S23	Query or set the Serial port configuration *Note: The serial port parameter is optional. If no serial port is specified, ATS23 queries or sets the serial port it is received on.* ATS23?[Serial port] to query • 0=Serial port on the device • 1=Serial port on the I/O X-Card, if installed on a GX device ATS23=[Baud,][Data bits, Parity, Stop Bits][,Serial port] to set Baud: • 300 • 1200 • 2400 • 4800 • 9600 • 19200 • 38400 • 57600 • 115200 Data bits: • 7 • 8 Parity: • O=Odd • E=Even • N=None • M=Mark Stop Bits: • 1 • 1.5 • 2 Serial port: • 0=Serial port on the device • 1=Serial port on the I/O X-Card, if installed on a GX device Example: ATS23=115200,8,N,2,0 (Sets the device to 115200, etc.) The settings take effect after reboot. *Note: Must be 8 data bits for PPP mode.*

Table D-11: Standard (Hayes) AT Commands (Continued)

Command	Description
S211	For applications or situations where hardware control of the DTR signal is not possible, the device can be configured to ignore DTR. When Ignore DTR is enabled, the device operates as if the DTR signal is always asserted. ATS211? to query ATS211=n to set • n=0—Use hardware DTR (default) • n=1—Ignore DTR • n=3—Ignore DTR and assert DSR.
S221	Query or set the Connect Delay—the number of seconds to delay the connect response when establishing a TCP connection. ATS211? to query ATS211=n to set • n=0–255
V	Query or set the AT command responses (verbosity). ATV? to query ATVn to set • n=0 — Numeric (terse) command responses (The numeric responses follow the Hayes Standards for commands.) • n=1 — Text string (verbose) command responses (default) *Note: Do not use an equal sign (=) when issuing the command.*
&V	Lists most AT commands and their current values. If the parameter is not configured, the AT command returns “Not Set”.
&W	Saves the settings for parameters that are temporarily set without being permanently written to the memory. This command does not apply to ALEOS because once you issue an AT command or change a setting in ACEmanager and click Apply, the changes are saved in non-volatile memory and are persist across reboots.
X	Query or set the Extended Call Process Result mode ATX? to query ATXn to set • n=0 — No extended code (default) • n=1 — Adds the text 19200 to the connect response
Z	Reboots the AirLink device. *Note: If *DATZ is set to 1, Z is blocked. See *DATZ on page 438.*

I/O

Table D-12: Input/Output AT Commands

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>*ANALOGIN[n]?</td><td>Query individual analog input values (in volts).
AT*ANALOGIN[n]?
• n=1–4

Note: Four analog inputs are available on an AirLink GX Series device with an I/O X-Card installed. To confirm that an I/O X-Card is installed, check the X-Card Type field on Status > Home.
One analog input is available on the AirLink LS300.</td></tr>
<tr><td>*DIGITALIN[n]?</td><td>Query individual digital inputs. The digital inputs report either a 0 (open) or 1 (closed).
AT*DIGITALIN[n]?
• n=1–5 (Input number)

<table><tr><th>Volts</th><th>Digital value</th></tr><tr><td>-0.5 – 1.2</td><td>0</td></tr><tr><td>1.3 – 30</td><td>1</td></tr></table>
Note: Digital inputs 2, 3, 4, and 5 are only available on an AirLink GX Series device with an I/O X-Card installed. To confirm that an I/O X-Card is installed, check the X-Card Type field on Status > Home.</td></tr>
<tr><td>*PULSECNT[n]?</td><td>Query the I/O pulse counts for digital in.
AT*PULSECNT[n]?
• n=1–5

Note: Pulse counts 2–5 are only available on a GX Series device with an I/O card installed.</td></tr>
<tr><td>*RELAYOUT[#]</td><td>Query or set the relay status.
AT*RELAYOUT[#]? to query
AT*RELAYOUT[#]=n to set
• # = 1–5
• n=0—OFF
• n=1—Drive Active Low

Note: Relay outputs 3, 4, and 5 are only available on an AirLink GX Series device with an I/O X-Card installed. To confirm that an I/O X-Card is installed, check the X-Card Type field on Status > Home.</td></tr>
</table>

Applications

Table D-13: Applications > Data Usage Commands

Command	Description
***DATACURDAY?**	Display data usage for the current day (in KB).
***DATAPLANUNITS**	Query or set the units for the data usage report AT*DATAPLANUNITS to query AT*DATAPLANUNITS=n to set • n=1—Sets the units to Megabytes (MB) • n=2—Sets the units to Kilobytes (KB)
***DATAPREVDAY?**	Query the data usage for the previous day (in KB).
***DATAUSAGEENABLE**	Query or set enabling Data Usage. AT*DATAUSAGEENABLE? to query AT*DATAUSAGEENABLE=n to set • n=0—Data Usage disabled • n=1—Data Usage enabled
***GARMINATTACH**	Query or set the ability to connect a Garmin device to the serial port (so the Garmin device can communicate with a remote server). For more information, see Garmin on page 311. AT*GARMINATTACH? to query AT*GARMINATTACH=n to set • n=0—Disable • n=1—Enable
***GARMINSTATUS?**	Query Garmin device attachment status.

Table D-14: Applications > ALEOS Application Framework (AAF)

Command	Description
***AAFINSTALL**	Query installed AAF applications and their status and install new AAF applications • AT*AAFINSTALL? returns the installation status of the last installed application, and list of installed AAF applications and the status of each application. • AT*AAFINSTALL?<application name> returns the status of the specified AAF application. • AT*AAFINSTALL=<hostname>,<user>,<password>,<application filename> downloads and installs the specified AAF application from the FTP server at <hostname> using <user> <password> credentials.
***AAFUNINSTALL**	Install an AAF application AT*AAFUNINSTALL=<application name> uninstalls the specified AAF application.

Admin

Table 4-15: Admin > Advanced Commands

Command	Description
***BLOCK_RESET_CONFIG**	Query or set the ability to block resetting the device to factory default settings using the hardware Reset button. AT*BLOCK_RESET_CONFIG? to query AT*BLOCK_RESET_CONFIG=n to set • n=0—Reset button can be used to reset the device to factory default settings. (default). • n=1—Device cannot be reset to factory default settings using the Reset button on the device. *Note: This command only blocks the ability to reset to defaults using the Reset button on the device. You can still reset the device to the factory default settings using the "Reset to Factory Default" button in ACEmanager or the *RESETCFG AT command.*
***BOARDTEMP?**	Query the temperature of the internal hardware, in degrees Celsius.
***DATE?**	Query the internal clock. The date and time are always specified in a 24-hour notation. AT*DATE? to query *Note: In AirLink devices, the GPS and/or cellular connection is used to set the time.*
***MSCIUPADDR**	Query or set the IP address or FQDN and port that periodic device status updates are sent to. AT*MSCIUPADDR[IP address or FQDN][/port]? to query AT*MSCIUPADDR=[IP address or FQDN][/port] to set Examples: 192.168.14.100/3333 MyDevice.com/3333
***MSCIUPDPERIOD**	Query or set the device status update interval (in seconds). Thsi specifies how frequently the device status update is sent to the port configured in *MSCIUPADDR. AT*MSCIUPDPERIOD? to query AT*MSCIUPDPERIOD=n to set • n=0 — Disabled • n=1–255 seconds
NSLOOKUP	Immediately performs an NSLookup on the supplied FQDN. ATNSLOOKUP=[FQDN]
***POWERIN?**	Query the voltage input to the internal hardware.

Table 4-15: Admin > Advanced Commands

Command	Description
***RESETCFG**	AT*RESTCFG resets the device to factory default settings. **Important:** *There is no confirmation requested. The AT command takes effect immediately.*
***REMOTELOG**	Exports the log file to a remote destination (Syslog Server). Specifying the port is option. If the port is not specified, the default port, 514, is used. You can only use this command locally. AT*REMOTELOG=SYSLOG SERVER IP,PORT

***SECUREMODE**	Query or set the secure mode that blocks most ports (and ICMP) for over-the-air (OTA) or OTA and local to prevent unwanted access to the device.
	AT*SECUREMODE? to query
	AT*SECUREMODE=n to set
	• n=0 Off; normal behavior
	• n=1 Disables:
	  • Web management ports (ACEmanager and AVMS access) from the OTA interface
	  • Internet Control Message Protocol (ICMP), used for PING, for OTA and Wi-Fi
	• n=2 Disables:
	  • Web management ports from the Over-the-air (OTA) interface
	  • Internet Control Message Protocol (ICMP) for OTA and Wi-Fi
	  • ICMP for local ports (Ethernet, USB, and Serial)
	
	Note: Telnet and SSH ALEOS ports remain open regardless of the secure mode setting. This enables you to connect an AT console to manage the device. DHCP and DNS ports also remain open to allow the device to provide IP addresses to hosts and relay the DNS service.

***SYSRESETS?**	Query the number of resets since the device was reset to factory default settings.
***USBBYPASS**	Query or set Radio Passthru mode. AT*USBBYPASS? to query AT*USBBYPASS=n to set • n=0—Disable • n=1—Enable

E: SMS Commands

SMS Command format

PW [Password] [Prefix][Command or Command parameter1] [Command parameter2 (if applicable)] [Command parameter n]

Note: There is no space between the prefix and the command (or the 1st command parameter in the case of multi-parameter commands). There must be a single space between all other fields to act as a delimiter.

The default password is the last 4 digits of the SIM ID number (for SIM-based devices) and the last 4 digits of the ESN (for non-SIM devices). If you do not know the SIM ID or ESN number, you can find it in ACEmanager on the Status > WAN/Cellular page.

The default prefix is “&&&”.

Whether or not a password and prefix are required varies depending on the SMS mode selected in ACEmanager.

SMS mode	Password (configurable in all modes)	Prefix
Password Only	Always required	Required Use default (not configurable)
Control Only	Required when sending from a non-trusted phone number	Prefix is configurable. The prefix can be omitted if the ALEOS Command Prefix field in ACEmanager (Services > SMS) is configured to be blank.
Gateway Only	Always required	Required Use default (not configurable)
Control and Gateway	Required when sending from a non-trusted phone number	Required Configurable, but cannot be blank

When an SMS command is received, the AirLink device performs the action requested and sends a response back to the phone number from which it received the SMS.

For more examples and detailed instructions, see SMS Overview on page 198.

List of SMS Commands

Command	Action	Result
Note: Some responses start with "reply from [device name]:" However, this feature is currently unavailable for the Enable, and Provision commands.		
[prefix]enable <value>	Enable/disable the device(s) being managed by AVMS.	"AVMS enable set to status:" <value> <value>=0 Disable <value>=1 Enable
[prefix]status	None	status IP [Network IP] [Network Status]: [technology type] RSS signalled Lat = [Latitude] Long = [Longitude] Time = [hh:mm:ss]
[prefix]reset	Resets the device 30 seconds after the first response message is sent.	First message: Reset in 30 seconds Second message: Status message when back up.
[prefix]relay x y	Sets the applicable relay to the desired setting.	relay x set to y x can be 1 y can be 0 or 1 (Off or Drive active low)
[prefix]GPS	The device replies with its current GPS location.	The device sends a link to a map showing its location. You can copy the link into a browser to view the location, or if the SMS is sent from a smartphone, you can click the link to view the map.
[prefix]Provision <APN> <Network User ID> <Network Password> *Note: You can omit any of the above fields by using a leading or single period (.) for that parameter.* *Note: Use of this command is valid for LTE, HSPA, and GPRS networks, but not valid for CDMA only networks.*	After the unit is installed and the SIM card inserted, you can use this command to provision the account.	"provision" "apn:" <APN> "user ID" <Network User ID> "PW" <Network Password>

Command	Action	Result
[prefix]AVMS <server> <interval> *Note: All of the above must be on a single line. The interval must be greater than 0. Omitting any field results in a response of "not set" and the configuration parameter does not change.*	Modifies the AVMS server's URL and AVMS communication period (interval in minutes)	"AVMS" "srv:" <Server> "interval:" <Interval>
[prefix]AVMSCHECKIN	Prompts the device to communicate with the AVMS server. Once AirVantage Management Service receives the heartbeat message, it can respond and send an MSCI command to the device (i.e Write/Read/ Firmware Update).	"AVMS connection requested"

F: Q & A and Troubleshooting

F

ACEmanager Web UI

The ACEmanager page is not displaying properly.

1. Ensure the you are using a supported browser. See page 17 for a list of supported browsers.
2. Hold the Shift key + click the Refresh button. This reloads the page, while ignoring what is in the cache.

If the problem persists:

- Clear the cache. (The procedure varies, depending on the browser.)
- Restart the browser.
- Restart your computer.

Ethernet Ports

My GX Series device has a Ethernet X-Card installed, but the ports are not working, and the Ethernet LEDs are not lit.

1. Launch ACEmanager.
2. Go to the LAN tab.
3. Select DHCP/Addressing in the menu on the left of the screen.
4. In the Host Connection Mode field, ensure that Ethernet Uses Public IP is not select.

If “Ethernet Uses Public IP” is selected in the Host Connection Mode field, the Ethernet ports are disabled.

What do the LEDs above the Ethernet port mean?

There are two LEDs at the top of the Ethernet port. The green on is lit when there is a cable connected to the host and the connection is running at 100baseT. The amber (activity) LED blinks when traffic is passing through the port.

LAN Networks

The server on my LAN network is receiving data from some hosts on the network, but not others. What's wrong?

If you have a network with multiple LAN hosts that are sending data to the same server and the server is not receiving data from one (or more) of the hosts, it may be because the Mobile Network Operator has a WAN firewall that is blocking the ports used by the NAT for over-the-air (OTA) destinations.

To correct this problem:

1. Launch ACEmanager.
2. Go to the LAN/Wi-Fi tab.
3. Select Ethernet.
4. Refer to the instructions for setting the Starting Ephemeral Port on page 119.)

Wi-Fi

My GX Series device has a Wi-Fi X-Card installed, and I have it configured to act as an access point, but I don't see an option to use WEP encryption.

1. Launch ACEmanager.
2. Go to the LAN/Wi-Fi tab.
3. Select Wi-Fi.
4. In the Enable Access Point field, change the value from "b/g/n Enabled" to "b/g Enabled".

   Once this change is made, an "Open WEP" section appears below the Wi-Fi Configuration section.

WEP encryption is only supported on 802.11b and 802.11g. It is not supported on 802.11n.

Port Forwarding

I set up port forwarding rules. I did not receive an error message, but it seems that data is not being forwarded.

If the Public Start Port and Public End Port fields are not set up correctly, data is not forwarded.

1. In ACEmanager, go to Security > Port Forwarding.

- If you are forwarding data to a single port:
  - Ensure that the value in the Public Start Port field is **not** 0.
  - Ensure that the value in the Public End Port field **is** 0.
  - Ensure that the value in the Private Port start field is **not** 0.
- If you are forwarding data to a range of ports:

1. Ensure that the value in the Public Start Port field is not 0.

- Ensure that the value in the Public End Port field is greater than the value in Public Start Port field.
- Ensure that the value in the Private Port Start field is not 0.

For complete instructions, see Port Forwarding on page 169.

ALEOS Application Framework (ALEOS AF)

I'm unable to load an application from ALEOS AF.

1. In ACEmanager, go to Services > Telnet/SSH.
2. In the AT Server Mode field, select Telnet.
3. Click Apply.
4. Re-try loading the application from ALEOS AF.

SMS

I tried to send an SMS message, and received an error code. What does the error code mean?

The following acknowledgment error codes may appear if your message was not successfully sent:

Code:	Explanation:
100	Not in coverage (no cellular service)
201	Parse Error on field #1 (Start Field)
202	Parse Error on field #2 (Phone number and separator)
203	Parse Error on field #3 (Data type and separator)
204	Parse Error on field #4 (Payload length and separator)
205	Parse Error on field #5 (Message and End Field)
301	No buffers available
302	SMS queue full

Supported SMS data types are ASCII, 8-bit, and Unicode, and are all case-sensitive. SMS messages being sent MUST be in ASCII hex format.

I tried to send an SMS command and received the error "not set". The parameter was not changed.

Check the format of the SMS command. There should be no space between the prefix and the command (or the 1st command parameter in the case of multi-parameter commands), and a single space between all other fields to act as a delimiter. For more information, see SMS Commands on page 447 and SMS Overview on page 198.

GPS

I set the GPS Reports Port field on the GPS > Local Streaming page to stream GPS data to a USB port, but I don't see GPS data on the USB port.

The GPS streaming feature works with serial devices. To stream data to a USB port, you must first configure the USB port to act as a serial device.

1. In ACEmanager, go to the LAN > USB tab.
2. In the USB Device Mode field, select USB Serial.
3. Click Apply.

If you have not already done so:

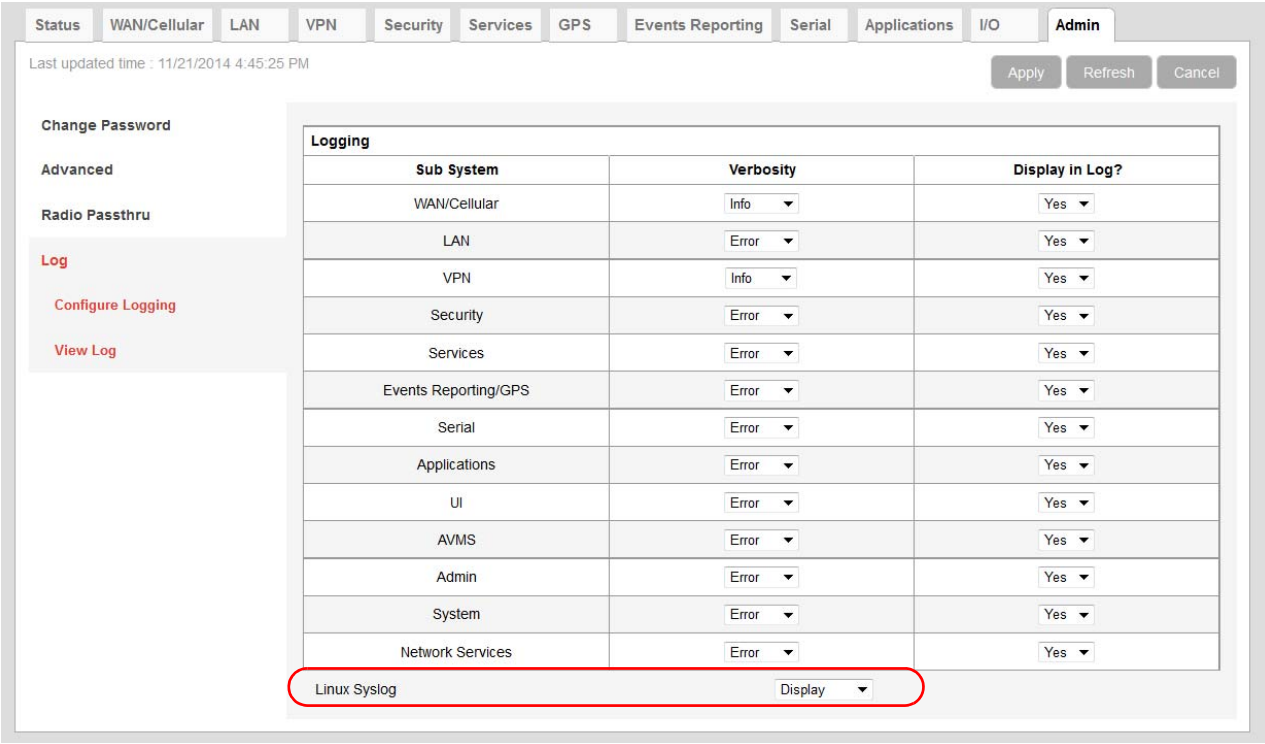
1. Go to GPS > Local Streaming.
2. In the GPS Reports port field, select one of the following:
   - USB Serial
   - DB9 and USB
3. Click Apply.
4. After you have made all the configuration changes, reboot the device.

VPN

My VPN connection is not working. When I try to debug it using the logs on the Admin page, VPN information does not show up in the log.

VPN information is collected in the Linux logs. To view this information:

1. Log into ACEmanager as User and go to Admin > Log.



2. In the drop-down menu beside Linux Syslog, ensure that Display is selected. If you change the setting:
   a. Click Apply.
   b. Reboot the device.
3. Click View Log.
4. On the View Log page, click Clear and then click Refresh.

VPN Troubleshooting

If you see the following lines in the log, it means the VPN Server is not answering.

```
notice openvpn[9199]: [UNDEF] Inactivity timeout (--ping-restart), restarting
notice openvpn[9199]: TCP/UDP: Closing socket
```

Check the VPN Server status.

When I configure a VPN, my Internet connection stops working.

When you configure a VPN, outgoing traffic from the host to the public Internet is blocked by default, as a security measure. If you want to enable public Internet traffic from the host:

1. In ACEmanager, go to VPN > Split Tunnel.
2. Change the Outgoing Host Out of Band field to Allowed.
3. Click Apply.

Poor Wireless Network Connection

ACE manager indicates that my AirLink device has a poor wireless connection. What can I do to improve it?

For GSM or CDMA networks:

1. Check the RSSI value. If ACEmanager (Status screen) indicates a good RSSI value, go to step 2. If it indicates a poor RSSI value:
   - Check the antenna connection.
   - Make sure you have the correct antenna for the device.
   - You may be in an area with poor coverage. Check with your Mobile Network Operator, or if possible, try moving the AirLink device to a new location.
2. Check the Ec/Io value. If ACEmanager (Status screen) indicates a poor Ec/Io value:
   - This may be a temporary network problem caused by local interference.
   - A nearby laptop or other electronic equipment may be interfering with the signal. Try moving the AirLink device to a different location.

For LTE networks:

1. Check the RSSI value. If ACEmanager (Status screen) indicates a good RSSI value, go to step 2. If it indicates a poor RSSI value:
   - Check the antenna connection.
   - Make sure you have the correct antenna for the device.
   - Try moving the AirLink device to a different location.
2. Check the RSRP value. If ACEmanager (Status screen) indicates a good RSRP value, go to step 3. If it indicates a poor RSRP value:
   - This may be a temporary network problem caused by local interference.
   - Check the antenna connection.
   - Make sure you have the correct antenna for the device.
   - You may be in an area with poor coverage. Check with your Mobile Network Operator, or if possible, try moving the AirLink device to a new location.
3. Check the RSRQ value. If ACEmanager (Status screen) indicates a poor RSRQ value:
   - A nearby laptop or other electronic equipment may be interfering with the signal. Try moving the AirLink device to a different location.

Connection not working

My device appears to be connected to the host, but no data is being transferred.

1. Check to see if MAC filtering is enabled (Security > MAC Filtering).
2. If MAC filtering is enabled:

- Ensure that the MAC Address for the host in question is on the Allowed List.
- Ensure that there are no typos in the MAC Address.

  Or

- If it is not required, disable MAC Filtering and reboot the device.

My host device is unable to connect to the Internet, even when there is good cellular network coverage and ALEOS can Ping an external IP address.

1. Check the DNS proxy setting described on page 140.

   You may need to change this setting to Disable so that all connected hosts acquire the Mobile Network Operator-defined DNS server as the first DNS server. The AirLink device is not used as the DNS resolver.

Updating the ALEOS Software and Radio Module Firmware

I am unable to update the ALEOS software and radio module firmware using ACEmanager.

If you are having trouble updating the ALEOS software or radio module firmware, especially if you are updating from an older version of ALEOS:

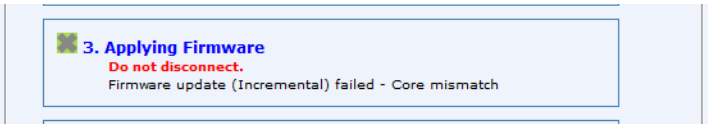
1. Try using a different browser. (ACEmanager supports the latest versions of Internet Explorer and Firefox.)
2. Delete the browser cookies/cache before logging into ACEmanager. (The Web browser short-cut is Control + Shift + Delete.)
3. Backup your device settings by downloading and saving the template. See Saving a Custom Configuration as a Template on page 19.
4. Reset the device to factory default settings. (See Reset to Factory Default on page 327 or press and hold the reset button on the device for 7 to 10 seconds.)
5. If you are updating from ALEOS 4.3.3 or earlier, be sure to follow the correct software update path. For more information, refer to the Upgrading to ALEOS 4.3.4 from Older Versions Application Note (part number 4115254) available on www.sierrawireless.com/Support/Downloads.aspx.
6. Begin the update process (see Update the ALEOS Software and Radio Module Firmware on page 30) and follow the prompts.
7. If after 30 minutes the Web UI is frozen, log in using a different browser and confirm whether or not the ALEOS software and radio module firmware has been updated correctly.
8. If you are still having problems, contact your Sierra Wireless distributor.

When I am trying to update the radio module firmware, the connection times out and I cannot reconnect to the device.

Depending on the file size and the connection speed, it can take 10 to 20 minutes to upload and install the radio module firmware. While this is taking place, you may see a “connection timed out” message. You can ignore this message, as the connection is still valid and the firmware update process is continuing. If you are connected to the device over-the-air, you will not be able to access the device until the radio module update is complete.

1. Continue to wait for the process to complete and the device to reboot.
   - **Do Not** reset the device.
   - **Do Not** disconnect the power.
   - **Do Not** click Cancel.
2. If after 20 minutes, the device does not reboot, contact Sierra Wireless Technical Support.

When I try to update ALEOS using ACEmanager, I see the following message: “Firmware update (Incremental) failed - Core mismatch”.

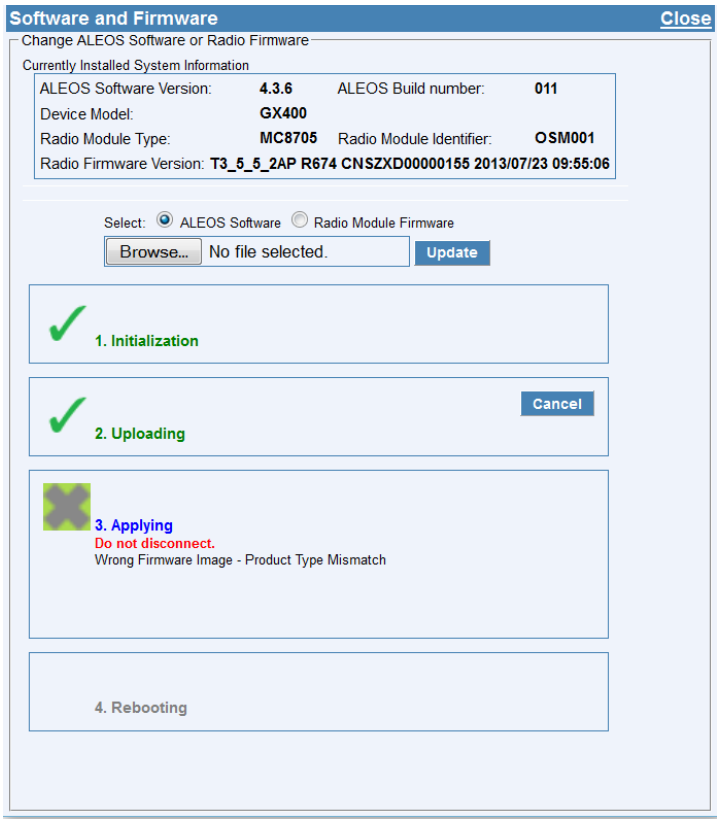


This message appears when the device you are trying to update the AirLink device with an Incremental ALEOS version.

To correct the problem:

1. Click Cancel.
2. Close ACEmanager.
3. Ensure that you have downloaded the correct ALEOS version for your device and Mobile Network Operator.
4. Re-launch ACEmanger, log in, click the Firmware link, and retry the Software and firmware update.

When I try to update ALEOS using ACEmanager, I see the following message: “Firmware update failed - Bad image”.

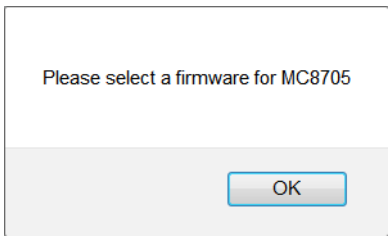


This message also appears if you are only updating the radio module firmware and you have the Update ALEOS radio button selected.

To correct the problem:

1. Close the Update page.
2. Retry the radio firmware update, being careful to select the Radio Module Firmware button before clicking Browse.

When I try to update ALEOS using ACEmanager, I see the following message: “Please select a firmware for xxxx”.



This message appears and you are blocked from continuing with the update if you are only updating the radio module and you select a radio module firmware file designed for a different radio module.

To correct the problem:

1. Click OK.
2. Select a radio module firmware file for the radio module in the AirLink device you are updating and click update. (To check which radio module is in your device, in ACEmanager, go to Status > About.)

When I try to update the radio module using AVMS, I receive an error message.

The following table provides a brief explanation of the firmware update error messages.

Error message	Meaning	Corrective action
Cannot Install Firmware	The system has encountered errors from which it cannot recover and requires at least a reboot before trying to update again.	1. Reboot the device. 2. If the problem persists, press the reset button for 7–10 seconds to reset the device to the factory default settings (release the reset button when all four LEDs turn from red to yellow) and try again. 3. If it still does not work, contact AVMS support[a].
Link not up in 3 minutes...Exiting	The radio module was not able to establish the connection in 3 minutes. The update has been aborted, but can be relaunched as soon as the connection is OK.	Wait for network connectivity and then try again.
Unable to download JUD file from <url>	The URL is wrong, or the download failed (interruption, no space left...).	Contact AVMS support[a].
Core version not found in JUD file	JUD file is not valid. Core Version is a mandatory field.	There is a problem with the package on the AVMS server. Contact AVMS support[a].
Required information (URL, Size or MD5) is missing from JUD file	JUD file is not valid. URL, Size, and MD5 sum of the firmware package are mandatory fields.	There is a problem with the package on the AVMS server. Contact AVMS support[a].
Cannot perform upgrade — No space left on device	Firmware is larger than available space for the download.	Contact AVMS support[a]. The support team will need to access the device to clear space, or you can return the device to Sierra Wireless under an RMA.
Unable to download ALEOS firmware from <url>	Firmware URL is not valid, or the download failed.	Retry. If the download fails several times, contact AVMS support[a]. The support team will need a log from the device.
Undefined ALEOS firmware URL	ALEOS firmware URL not specified, so firmware cannot be retrieved.	Contact AVMS support[a] to confirm that there is not a problem with the service.

Error message	Meaning	Corrective action
ALEOS firmware MD5 check failed	The downloaded firmware package failed the integrity check. The update is aborted.	There is a problem with the package on the device or the download may have failed. Restart the firmware download. If the problem persists, contact AVMS support[a]. There may be a problem with the package on the AVMS server.
Unable to apply ALEOS firmware and Unable to apply ALEOS firmware (retry)	ALEOS firmware could not be applied. Check the ALEOS log messages to determine exactly why the update failed.	Retry. If the problem persists, contact AVMS support[a] and provide them with the log messages.
Radio Module URL is missing from JUD file	JUD file is not valid. The Radio Module Firmware URL is a mandatory field.	There is a problem with the package on the AVMS server. Contact AVMS support[a].
Radio Module package MD5 sum is missing from JUD file	JUD file is not valid. The Radio Module Firmware MD5 sum is a mandatory field.	There is a problem with the package on the AVMS server. Contact AVMS support[a].
Radio Module firmware MD5 check failed	The downloaded firmware package failed the integrity check. The update is aborted.	There is a problem with the package on the device or the download may have failed. Try downloading the file again. If the problem persists, contact AVMS support[a]. There may be a problem with the package on the AVMS server.
Radio Module backup failed	The radio module was saved to prevent a power failure. If the firmware cannot be backed-up on persistent storage, the firmware update will not proceed because of the risk that the radio module update will not be able to finish if interrupted.	Contact AVMS support[a]. The support team will need to access the device to clear space, or you can return the device to Sierra Wireless under an RMA.
Radio Module firmware download failed	Firmware URL is not valid, or download failed.	Retry several times. If the problem persists, contact AVMS support[a]. The support team will need a log from the device.
Undefined Radio Module firmware URL	The URL cannot be retrieved. The update is aborted.	Retry. If the problem persists, contact AVMS support[a].
Radio Module firmware update failed	Radio module firmware could not be applied. Check the ALEOS log messages to determine exactly why the update failed.	Retry. If the problem persists, contact AVMS support[a].

a. AVMS technical support: https://issues.m2mop.net

TCP Connections

I went to the TCP section of the Serial screen and configured ALEOS to include the Device ID in TCP connections, but I get the message “Device ID Not Set”.

Setting the TCP connection to include the Device ID is a two step process:

1. In ACEmanager, go to Serial > TCP and ensure that the Include Device ID on TCP Connect field is set to Enable.

   (See Port Configuration on page 275.)

2. Go to GPS > Global Settings > General and configure the Use Device ID in Location Reports field. (See Global Settings on page 253.)

To confirm that the Device ID is configured, check the Status > About screen. The Device ID, if set, appears in the GPS/RAP Device ID field.

AirVantage Management Service

I don't understand the message that appears in the Status field in the Services > AVMS page.

The error messages in the Services > AVMS > Status field can be due to a communication failure, a problem with the AVMS server, or a failure when parsing a valid AVMS server response. The following table describes the error messages and the corrective action.

Error message	Meaning	Corrective action
Communication Failure Errors		
[HTTP] Initialization error	The transfer object could not be initialized.	Contact AVMS support[a].
[HTTP] Unsupported protocol	The AVMS server URL protocol is not supported.	In ACEmanager, check the AVMS URL in the Service > AVMS > Server URL field. The default value is http://na.m2mop.net/device/msci/com.
[HTTP] Failed initialization	The transfer library could not be initialized.	Contact AVMS support[a].
[HTTP] URL using bad/illegal format or missing URL	The AVMS server URL is missing or not properly formatted.	In ACEmanager, check the AVMS URL in the Service > AVMS > Server URL field. The default value is http://na.m2mop.net/device/msci/com.
[HTTP] Couldn't resolve host name	The AVMS server URL could not be resolved.	In ACEmanager, check the AVMS URL in the Service > AVMS > Server URL field. The default value is http://na.m2mop.net/device/msci/com. Also check the cellular connectivity.
[HTTP] Couldn't connect to server	Connection to the AVMS server URL failed.	In ACEmanager, check the AVMS URL in the Service > AVMS > Server URL field. The default value is http://na.m2mop.net/device/msci/com. Also check the cellular connectivity.
[HTTP] Timeout was reached	The transfer timeout (equal to the communication period if defined or 5 minutes) expired.	Check cellular connectivity.
[HTTP] Server returned nothing (no headers, no data)	No data was received from the AVMS server.	Check cellular connectivity.
[HTTP] Unrecognized or bad HTTP Content or Transfer-Encoding	The AVMS server HTTP response contains a malformed content or transfer-encoding header field.	Contact AVMS support[a].
[HTTP] Out of memory	A memory allocation problem occurred.	Contact AVMS support[a].

Error message	Meaning	Corrective action
[HTTP] SSL peer certificate or SSH remote key was not OK	This message appears if you are using an HTTPS server URL, the SSL Verify Peer Certificate field is set to Enable, and the server SSL certificate validation fails. If this happens, communication with the AVMS server is terminated.	If you see this error message: 1. Check to see that you have a valid URL in the Server URL field. 2. Contact your IT Administrator, or if you want the traffic to go through without verifying the server certificate, change the setting in the Services > AVMS > SSL Verify Peer Certificate field (described on page 183) to Disable.
AVMS Server Errors		
[AVMS] HTTP error '500'	AVMS server reported error 500 in the HTTP response.	Refer to the available AVMS server documentation for a list of all possible error codes and their significance.
Error message indicating a failure when parsing a valid AVMS server response		
XML processing error	The content of a valid AVMS server response cannot be parsed.	AVMS server responses are mal-formatted. Contact AVMS support[a].

a. AVMS technical support: https://issues.m2mop.net

LTE Networks

How do I interpret the number shown in the Band Class field on the Status > WAN Cellular page for a device on an LTE network?

Use the following table to interpret the values in the LTE Band Class field in ACEmanager (STATUS > WAN Cellular).

Band Class number	Uplink frequency range (MHz)	Downlink frequency range (MHz)
120	1920–1980	2110–2170
121	1850–1910	1930–1990
122	1710–1785	1805–1880
123	1710–1755	2110–2155
124	824–849	869–894
125	830–840	875–885
126	2500–2570	2620–2690
127	880–915	925–960
128	1749.9–1784.9	1844.9–1879.9
129	1710–1770	2110–2170
130	1427.9–1452.9	1475.9–1500.9
131	698–716	728–746

Band Class number	Uplink frequency range (MHz)	Downlink frequency range (MHz)
132	777–787	746–756
133	788–798	758–768
134–135	Reserved for bands 15 and 16	
136	704–716	734–746
137	815–830	860–875
138	830–845	875–890
139	832–862	791–821
140	1447.9–1462.9	1495.9–1510.9
141–151	Reserved for bands 22 to 32	
152	1900–1920	1900–1920
153	2010–2025	2010–2025
154	1850–1910	1850–1910
155	1930–1990	1930–1990
156	1910–1930	1910–1930
157	2570–2620	2570–2620
158	1880–1920	1880–1920
159	2300–2400	2300–2400

How do I obtain and interpret SINR values for LTE networks?

You can use the AT*CELLINFO? command to obtain an SINR (Signal to Interference plus Noise Ratio) value. (See *CELLINFO2? on page 389.)

The values vary depending on the network characteristics and the AirLink device, but in general, a positive value provides usable throughput. The following table provides guidelines for interpreting SINR values.

SINR Value	Throughput
< 0	Poor
0 to 5	Fair
6 to 10	Good
> 10	Excellent

If the SINR value indicates poor throughput:

- Move the antenna away from noisy equipment.
- Move closer to the nearest cell tower line of sight, or further away from the interfering cell tower.

SIM Card is Blocked

My SIM card has a PIN number. I've entered the wrong PIN several times and now the SIM card is blocked.

AirLink products do not support Personal Unlocking Key (PUK) entry. However, if you need to unblock the SIM card:

1. Contact your Mobile Network Operator to obtain the PUK.
2. Remove the SIM card from the AirLink device and insert it in a cell phone that accommodates a MiniSIM (2FF) card.
3. Enter the PUK to unblock the SIM card and then return the SIM card to the AirLink device.

Note: Be careful when entering the PUK. You have a limited number of attempts to enter the correct PUK (generally 10) before the SIM card is permanently disabled and a new SIM card is required. If the PUK does not unblock the SIM card after the first few attempts, contact your Mobile Network Operator.

Remote connections

I cannot connect to the AirLink device remotely over the Mobile Network Operator's Private Network via the Web UI, although I can connect to it locally.

Some Mobile Network Operators' private networks have restrictions on the maximum transmission unit (MTU) size. This is more prevalent with LTE networks.

Possible solutions:

- Use your Mobile Network Operator's public network.
- Ask your Mobile Network Operator to reduce the MTU size on the router or other equipment at their end of the private network. Setting the MTU value below 1500 bytes (for example 1326 bytes) has resolved the problem on some private networks.
- If your AirLink device has a radio module (such as the MC7700 or MC7750) that supports LTE networks, select an option in ACEmanager (WAN/ Cellular > Advanced > Setting for Band field) that excludes LTE networks.

Radio Band Selection

I set the radio band in the UI (WAN/Cellular > Setting the Band) or by using the AT!BAND AT command, but after I reboot the band setting reverts to its former value.

For some SIM cards, you need to set the band before inserting the SIM card.

To resolve this problem:

1. Remove the SIM card.
2. Set the band to the desired value.

3. Reboot the device.
4. Insert the SIM card.

Reliable Static Routing (RSR)

I launched ACEmanager with Internet Explorer 9. I configured RSR, but after I enabled RSR and clicked Apply, all the values reverted to the defaults.

There is a known issue. If you configure and enable RSR with ACEmanager in Internet Explorer 9, and then click Apply, the values in the ACEmanager screen appear as default values.

This is an ACEmanager display issue only. The configuration is applied properly, but the configured values are not displayed. Click Refresh to view the configured values.

Inbound Ports Used by ALEOS

When I configure ports for an application on a LAN client such as a router or laptop, I want to ensure that the ports I use do not conflict with the inbound ports that ALEOS uses. Which ports does ALEOS use?

Table F-1 shows the inbound ports that are set in ALEOS and cannot be configured. Table F-2 show the default setting for ports you can configure and where to change the ports in ACEmanager.

Table F-1: ALEOS Non-configurable Inbound Ports

Port	Use
9494 – 9497 17335 17345 – 17353 21000 – 21003	Used internally for GPS and Events Reports
500 4500	Used internally for IPSec VPN
8088	Used internally for AVMS

Table F-2: ALEOS Configurable Inbound Ports

Default Port	Feature	ACEmanager location
161	SNMP Port	Services > Management (SNMP)
2332	SSH/Telnet Remote Login Server Port	Services > Telnet/SSH

Table F-2: ALEOS Configurable Inbound Ports

Default Port	Feature	ACEmanager location
9191	ACEmanager Port	Services > ACEmanager
9300	SSL tunnel Port	VPN > SSL Tunnel
9443	ACEmanager SSL Port	Services > ACEmanager
9494	GPS Poll Port	GPS > Global Settings
12345	Device Port used for incoming TCP/UDP traffic	Serial > Port Configuration
54321	X-Card Device Port used for incoming TCP/UDP traffic	Serial > I/O X-Card Configuration

Event Reporting

I set up ACEmanager to send an email/SMS report, but when I clicked the Test report button no report was sent.

After you set up the event reporting fields and click Apply, wait about a minute before you click the Test report button. The AirLink device needs this time to apply the new configuration.

I configured event reporting, but I did not receive a report when I should have.

- If the Action Type for the Event Reporting is Email or SNMP TRAP, be sure that these services are also configured on the Services tab.
  - To configure email, go to Services > Email (SMTP).
  - To configure SNMP TRAP, go the Services > Management (SNMP).
- If the Action Type is SMS, you may need to change the default settings in the Advanced section of the Services > SMS page.

TCP/IP and UDP/IP Auto Answer

I configured TCP/UDP auto answer, but the packet contents are not being streamed over the serial port to the connected device.

1. Try polling the device connected to the AirLink device's serial port.

   If you do not receive a response, confirm that the fields described in Configuring IP to Serial with Auto Answer and Serial to IP on page 298 are set correctly.
2. In ACEmanager, go to Status > Serial and check the Serial bytes sent field to confirm that packets are reaching the AirLink device from the mobile network and the packet contents are being sent out the AirLink device's serial port.

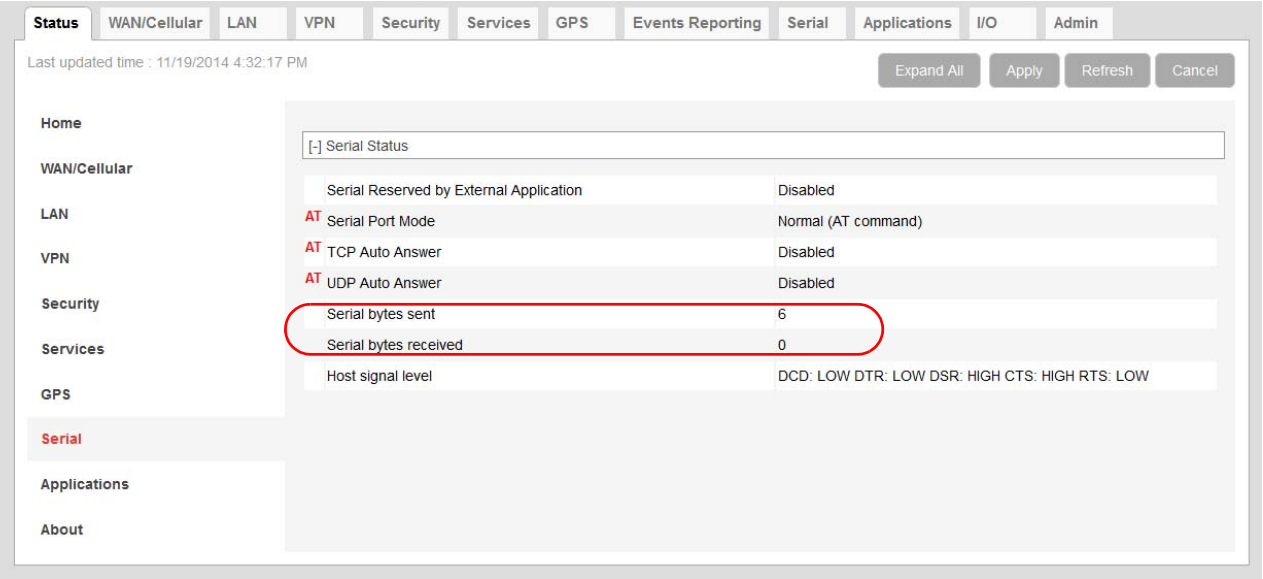


Figure 6-1: ACEmanager: Status > Serial

When you poll the AirLink device/connected device:

- If the Serial bytes sent counter increases, the IP packets have reached the AirLink device from the mobile network, the AirLink device has removed the header and sent the packet contents out its serial port to the connected device.
- If the Serial bytes sent counter does not increase, either:
  - The IP packet has not made it across the mobile network to the AirLink device.
  - The destination port for the TCP/IP or UDP/IP connection does not match the configured Device Port on the ACEmanager Serial tab.

3. Once you have confirmed that the Serial bytes sent counter is increasing, check the Serial bytes received counter (also on the Status > Serial screen).
   - If the Serial bytes received counter is increasing, the connected device is responding to the poll request and sending its response back to the AirLink device across the serial connection.
   - If the Serial bytes received counter is not increasing, the connected device is not responding to the poll request. Ensure that the serial cable is fully seated and properly connected to the AirLink device and the host. Check that you have the correct type of serial cable connecting the AirLink device to the connected device. The AirLink device is a DCE device. If the connected device is also a DCE device, use a null modem serial cable. If the connected device is a DTE device, use a straight through serial cable.
4. If you have confirmed that both the Serial bytes sent and Serial bytes received counters are increasing when you send a poll to the connected device, but you are still not receiving the response back on your original sending application, the most common reason is that the incoming packets from the AirLink device to your application are being blocked by a firewall on your network. The firewall may be blocking all traffic except packets destined for particular ports or arriving from particular ports.

Check with your firewall administrator. Ask the administrator to monitor the firewall when you poll the AirLink/connected device to see if any return packets from the AirLink device hit the firewall.

If you are still having problems, contact your Sierra Wireless distributor.

Templates

The template does not upload properly when I use Internet Explorer 9.

To resolve the problem:

1. In Internet Explorer 9, go to Tools > Internet Options.
2. Select the Security tab.

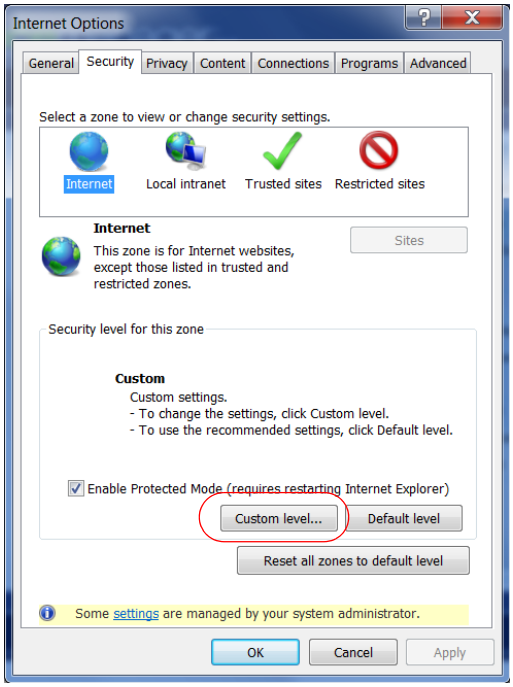


Figure 6-2: Internet Explorer 9: Tools > Internet Options > Security tab

3. Click Custom level....
4. Scroll down until you see “Include local directory path when uploading files to a server”.
5. Select Disable.

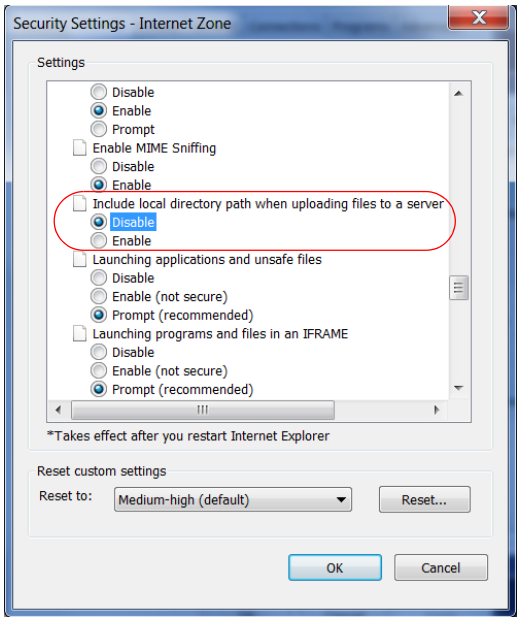


Figure 6-3: Internet Explorer 9: Security Settings

6. Click OK.

G: Glossary of Terms

G

Acronym or Term	Definition
1xEV-DO	Single Carrier (1X) EVolution–Data Only A high-speed standard for cellular packet data communications. It supports Internet connections with data rates up to 3.1 Mbps. (downlink from the network) and 1.8 Mbps (uplink to the network). Average data rates are approximately: • Rev. A: 600-1300 kbps. (downlink from the network) and 300-400 kbps (uplink to the network) • Rev. 0: 400-700 kbps (downlink from the network) and 40-80 kbps (uplink to the network) Actual speed depends on the network conditions. Compare to 1X.
1X	Single Carrier (1X) Radio Transmission Technology A high-speed standard for cellular packet data communications. 1x supports Internet connections with data rates up to 153 kbps (simultaneously in each direction—downlink and uplink). Actual speed depends on the network conditions. Compare to 1xEV-DO.
3GPP	3rd Generation Partnership Project 3GPP unites 6 telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TTA, TTC), and provides their members with a stable environment to produce Reports and Specifications that define 3GPP technologies.
API	Programming Interface A protocol intended to be used as an interface by software components to communicate with each other.
AT	A set of device commands, preceded by “AT” originally developed by Hayes, Inc. for their devices. The structure (but not the specific commands, which vary greatly from manufacturer to manufacturer) is a de facto device industry standard.
CDG	CDMA Development Group A consortium of companies who joined together to lead the adoption and evolution of CDMA wireless systems around the world. Also see CDMA.
CDMA	Code Division Multiple Access A wideband spread spectrum technique used in digital cellular, personal communications services, and other wireless networks. Wide channels (1.25 MHz) are obtained through spread spectrum transmissions, thus allowing many active users to share the same channel. Each user is assigned a unique digital code, which differentiates the individual conversations on the same channel.
cdmaOne	A IS-95 CDMA standard developed by QUALCOMM Inc. Also known as TIA-EIA-95.

Acronym or Term	Definition
CE, CE Label	The CE label is a mandatory conformity marking for products placed on the market in the European Economic Area (EEA). With the CE marking on a product, the manufacturer declares that the product conforms with the essential requirements of the applicable EC directives.
CnS	Sierra Wireless' proprietary Control and Status protocol interface
DCE	Data Communications Equipment A device that sits between the data terminal equipment (DTE) and a data transmission circuit. Usually the DCE is a modem.
Diversity	Antenna diversity, also called space diversity, is a scheme that uses two or more antennas to improve the quality and reliability of a wireless link. Often, especially in urban and indoor environments, there is no clear line-of-sight (LOS) between transmitter and receiver. Instead the signal is reflected along multiple paths before finally being received. Each bounce can introduce phase shifts, time delays, attenuations, and distortions that can destructively interfere with one another at the aperture of the receiving antenna.
EDGE	Enhanced Data rates for GSM Evolution A digital mobile phone technology that allows improved data transmission rates as a backward-compatible extension of GSM. EDGE is considered a pre-3G radio technology and is part of ITU's 3G definition. Also known as Enhanced GPRS (EGPRS), or IMT Single Carrier (IMT-SC), or Enhanced Data rates for Global Evolution.
EIA	Electronics Industry Association EIA was a standards and trade organization composed as an alliance of trade associations for electronics manufacturers in the United States. They developed standards to ensure the equipment of different manufacturers was compatible and interchangeable. The EIA ceased operations on February 11, 2011, but the former sectors continue to serve the constituencies of EIA.
EMC	Electromagnetic Compatibility The branch of electrical science which studies the unintentional generation, propagation and reception of electromagnetic energy with reference to the unwanted effects (Electromagnetic interference, or EMI) that such energy may induce.
EMI	Electromagnetic Interference The disturbance that affects an electrical circuit due to either electromagnetic induction or electromagnetic radiation emitted from an external source
ERP	Effective Radiated Power A standardized theoretical measurement of radio frequency (RF) energy. It is determined by subtracting system losses and adding system gains.
ESN	Electronic Serial Number The unique first-generation serial number assigned to the Air Link devices for use on the wireless network. Compare to MEID.
Ethernet	Computer networking technologies for local area networks (LANs).
EU	The European Union Organization of European countries.

Acronym or Term	Definition
EVDO	Enhanced Voice-Data Optimized or Enhanced Voice-Data Only (Ev-DO, EV, EVDO, etc.). A telecommunications standard for the wireless transmission of data through radio signals, typically for broadband Internet access. It uses multiplexing techniques including code division multiple access (CDMA) as well as time division multiplexing (TDM) to maximize both individual users' throughput and the overall system throughput.
FCC	Federal Communications Commission The U.S. federal agency responsible for interstate and foreign communications. The FCC regulates commercial and private radio spectrum management, sets rates for communications services, determines standards for equipment, and controls broadcast licensing.
FW	Firmware Software stored in ROM or EEPROM; essential programs that remains even when the system is turned off. Firmware is easier to change than hardware but more permanent than software stored on disk.
GPRS	General Packet Radio Service A packet-oriented mobile data service on 2G and 3G cellular communication systems. GPRS was originally standardized by European Telecommunications Standards Institute (ETSI) in response to the earlier CDPD and i-mode packet-switched cellular technologies. It is now maintained by the 3rd Generation Partnership Project (3GPP).
GPS	Global Positioning System A system that uses a series of 24 satellites to provide navigational data.
GSM	Global System for Mobile Communications (originally Groupe Spécial Mobile) GSM is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe protocols for second generation (2G) digital cellular networks used by mobile phones
HSPA	High Speed Packet Access An amalgamation of two mobile telephony protocols: High Speed Downlink Packet Access (HSDPA) and High Speed Uplink Packet Access (HSUPA). This extends and improves the performance of existing 3rd generation mobile telecommunication networks utilizing the WCDMA protocols.
HSPA+	Also called evolved HSPA This allows bit-rates to reach as high as 168 Mbit/s in the downlink and 22 Mbit/s in the uplink. An improved 3GPP standard.
IC	Industry Canada The government department responsible for overseeing and regulating wireless and communication technologies in Canada.
IEC	International Electrotechnical Commission A non-governmental international standards organization that prepares and publishes International Standards for all electrical, electronic and related technologies – collectively known as "electrotechnology."

Acronym or Term	Definition
IOTA	Internet Over The Air An automated feature, supported by some service providers, to perform account setup by making a connection to the CDMA network and using a secure Internet connection to download account parameters to the device.
IS	Interim Standard After receiving industry consensus, the TIA/EIA forwards the standard to ANSI for approval.
IS-95	A 2G mobile telecommunications standard using CDMA to send voice, data and signaling data (such as a dialed telephone number) between mobile telephones and cell sites.
ISAKMP	Internet Security Association and Key Management Protocol A security protocol defined by RFC 2408 for establishing Security Associations (SA) and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange and is designed to be key exchange independent.
ITU	International Telecommunication Union A specialized agency of the United Nations responsible for issues that concern information and communication technologies. The ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, and assists in the development and coordination of worldwide technical standards.
kbps	Kilobits per second 1000, not 1024, as used in computer memory size measurements of kilobytes.
LED	Light Emitting Diode A semiconductor diode that emits visible or infrared light.
LTE	Long Term Evolution High performance air interface for cellular mobile communication systems.
Mbps	Millions of bits per second, or Megabits per second.
MEID	Mobile Equipment IDentifier The unique second-generation serial n umber assigned to the device for use on the wireless network. *Compare to* ESN.
MSCI	Modem Status Configuration Interface ALEOS internal configuration database
NAM	Number Assignment Module Semi-permanent information stored in the device's non-volatile memory, including the device's Mobile Identification Number, the station class mark, Mobile Network Operator code, and other cellular identifiers. Essentially the phone number, it should be treated as confidential information and should not be disclosed to anyone other than the cellular service provider.
NV	Non-Volatile (memory)
OEM	Original Equipment Manufacturer A company that manufactures a product and sells it to a reseller.

Acronym or Term	Definition
OTAPA	Over the Air Parameter Administration A way of distributing new software updates or configuration settings to devices like cellphones and set-top boxes.
OTASP	Over the Air Service Provisioning. Also see OTAPA.
PCS	Personal Communications Services A cellular communication infrastructure that uses a different frequency range than AMPS.
PPP	Point to Point Protocol An alternative communications protocol used between computers, or between computers and routers on the Internet. PPP is an enhanced SLIP. Also see SLIP.
PRI	Product Release Instructions A file containing the settings used to configure devices for a particular service provider, customer, or purpose.
RF	Radio Frequency
RoHS	Restriction of use of Hazardous Substances mandated by EU Directive 2002/95.
RS-232	A series of standards for serial binary single-ended data and control signals connecting between a DTE (Data Terminal Equipment) and a DCE (Data Circuit-terminating Equipment). It is commonly used in computer serial ports.
Rx	Receive
SIM, SIM Card	Subscriber identity module or subscriber identification module. An integrated circuit which securely stores the international mobile subscriber identity (IMSI) and the related key used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers).
SINR	Signal to Interference plus Noise Ratio (SINR) is an RF parameter that is directly proportional to throughput (the higher the number, the higher the throughput). It can help LTE radio installers gauge the signal quality between the cell tower and the radio module. For more information on interpreting the SINR values, see How do I obtain and interpret SINR values for LTE networks? on page 464.
SKU	Stock Keeping Unit Identifies an inventory item: a unique code, consisting of numbers or letters and numbers, assigned to a product by a retailer for purposes of identification and inventory control.
SLIP	Serial Line Internet (or Interface) Protocol An Internet Protocol designed to work over serial ports and modem connections. On personal computers, SLIP has been largely replaced by the Point-to-Point Protocol (PPP), which has more features and does not require its IP address configuration to be set before it is established. On microcontrollers SLIP is still the preferred way of encapsulating IP packets due to its very small overhead. Also see PPP.
SMS	Short Message Service A feature which allows users of a wireless device on a wireless network to receive or transmit short electronic alphanumeric messages (up to 160 characters, depending on the service provider).

Acronym or Term	Definition
TIA/EIA	Telecommunications Industry Association / Electronics Industry Association A standards setting trade organization, whose members provide communications and information technology products, systems, distribution services and professional services in the United States and around the world.
Tx	Transmit
UMTS	Universal Mobile Telecommunications System (UMTS). A third generation mobile cellular system for networks based on the GSM standard. Developed and maintained by the 3GPP (3rd Generation Partnership Project), UMTS is a component of the International Telecommunications Union IMT-2000 standard set and compares with the CDMA2000 standard set for networks based on the competing cdmaOne technology.
USB	Universal Serial Bus An industry standard defining the cables, connectors and communications protocols used in a bus for connection, communication and power supply between computers and electronic devices.
X.509	A Public Key Infrastructure (PKI) and Privilege Management Infrastructure (PMI) are standards that specify formats for public key certificates, certificate revocation lists, attribute certificates, a certification path validation algorithm, etc.

Index

A

access points
  maximum number configurable for GX, 134
ACEmanager, 184
  configuring, 18
  description, 13
  idle timeout, set, 184
  login, 17
  overview, 13
ACEview, 352
ALEOS Application Framework
  troubleshooting, 453
  unable to load application from, 453
  using, 314
ALEOS software update, 30
always on connect, 82, 210
analog inputs
  channel configuration, 390
  transformed values, 322
  uses, 317
APN, 79
  backup, 96
  status, 52
applications, 303
  status, 72
AT Commands
  Applications > Data Usage, 443
  GPS > Server 1 - Server 4, 422
  I/O > Current State, 442
  LAN/Wi-Fi > DHCP/Addressing, 401
  Security > Trusted IPs - Inbound, 407, 412
  Serial > Port Configuration, 429
  Services > Low Power, 413
  Status > Home, 389, 436
  summary, 387
  using, 387
  Wi-Fi, 404
authentication
  general information, 226
  LDAP, 227
  RADIUS, 228
  TACACS+, 229
AVMS
  configuration, 181
  error messages, 460

B

Bands, LTE, 463
bandwidth throttle, 97
browser support, 17

C

configuration
  application, 303
  events reporting, 257
  GPS, 233
  LAN, 111
  logging, 330
  serial, 275
  services, 181
  VPN, 155
  WAN/Cellular, 75
  Wi-Fi, 111
Connection not working, 456
custom SSL certificate, 185

D

data usage, 303
Dead Peer Detection, 161
device status (about), 73
Device Status Screen
  configuring, 231
DHCP/Addressing, 112
Dial-up Networking, 333
digital inputs
  GX Series, 317
  LS300, 317
  uses, 318
DMNR, 105
DMZ, 173
DNS
  alternate port, 141
  dynamic, 191
  global, 139
  override, 140
DNS proxy
  configure, 140
  status, 50, 53
documentation, 14, 15
domain name, 196
dual mode Wi-Fi, 138
DUN
  operating systems supported, 333
  setting up, 333
Dynamic Mobile Network Routing *See* DMNR

E

EC/IO, 47
email
  SMTP, 218
  test, 215
engine hours, 272

Ethernet
and DMZ, 174
and host connection mode, 114
AT commands, 390
MAC address, 73
status, 62
troubleshooting, 451
troubleshooting LEDs, 451
virtual port, 123
Ethernet ports, 117
troubleshooting, 451
events reporting configuration, 257

F

firmware update, 30

G

Garmin, 311
global DNS, 139
Glossary, 471
GPS
configuration, 233
global settings, 253
local IP report, 249, 252
status, 68
streaming, 454
troubleshooting, 454
GRE, 162

H

Host Interface Watchdog, 152
host port routing, 37, 128

I

Idle timeout, ACEmanager, 184
inbound ports used by ALEOS, 466
Internal DHCP Server, 115
IP Manager, 194
IPsec, 157
IPv6
cellular address (LTE, fallback to EV-DO), 56
cellular address LTE, fallback to HSPA), 59
configuring support for, 84, 88
prefix length (LTE, fallback to EV-DO), 56
prefix length (LTE, fallback to HSPA), 60

K

keepalive, 92

L

LAN
configuration, 111
management, 37
status, 62
LAN / Wi-Fi
status, 63
LDAP authentication, 227
LED indicator for serial traffic, 275
LEDs, above Ethernet port, 451
Load Root Certificate, 166
Local/Streaming, 247, 250
Log, mark a section of the log, 329
logging configuration, 330
login, 17
low power mode, 186
LTE Active Rescan, 90
LTE Active Reselection, MC7700, MC7710, 90
LTE Active Reselection, MC7750, 86
LTE Band Class field, 463

M

MAC filtering, 178, 456
MIB (Management Information Base), 361
Modbus, 289, 355
Modbus address list, 289
Modbus TCP/IP, 356

N

network connection, poor, 456
network settings, retain over reset, 328
Network State, 45
Network Watchdog, disable, 80, 81
NMEA, 234

O

Over the Air (OTA) connections, 38

P

PAD mode, 23
password, change, 325
PCI compliance, 38
ping, on demand, 327
port filtering
inbound, 175
outbound, 176
port forwarding, 169
error message, 452
troubleshooting, 452
PPP connection, configuring, 288
PPPoE, 141
Programmable Logic Controller, 356

public and private mode, 111
pulse count, 320

R

radio band, selecting, 81, 465
radio module firmware update, 30
radio passthru, 329
RADIUS authentication, 228
RAP, 234
re-activation, 96
redundant server, 245
relay outputs, 318
Reliable Static Routing (RSR), 100
Remote Terminal Unit, 355
reset device, retain network settings, 328
reset, periodic and time of day, 327
reverse telnet/SSH, 279
RSCP, 47
RSRP, 46
RSRQ, 47
RSSI, 46

S

security
  configuration, 169
  status, 66
serial
  status, 69
serial configuration, 275
serial port
  port configuration, 277
  PPP, 289
  TCP, 284
  UDP, 286
  virtual, 125
services
  status, 67
services configuration, 181
Simple Network Management Protocol (SNMP), 220
SINR, 464
SMS, 198
  advanced, 214
  Control Only mode, 201
  Gateway Only mode, 202
  M2M, 216
  Password, 213
  Password Only mode, 200
  password, default, 214
  Quick Test, 215
  security, 211
  test, 215
  troubleshooting, 453
  trusted phone number, 212
SMS Commands, 447
SMS M2M, 216
SMS message error, 453
SMS Wakeup, 210
SNMP traps, 361
SNTP, 225
split tunnel, 156
SSH, 217
SSH PAD mode, 23
SSL tunnel, 163
Status
  About, 73
  Applications, 72
  GPS, 68
  Home, 41
  LAN, 62
  LAN/Wi-Fi, 63
  Security, 66
  Serial, 69
  Services, 67
  VPN, 65
  WAN/Cellular, 49

T

TACACS+ authentication, 229
TAIP, 234
TCP connection
  configuring, 284
  Device ID Not Set, 461
  settings, 294
  troubleshooting, 460
telemetry, 355
Telnet, 217
template
  applying, 21
  saving a custom configuration as, 19
test button, SMS/email, 215
third party services, 193
time (SNTP), 225
troubleshooting
  ALEOS AF, 453
  AVMS error messages, 460
  AVMS status messages, 462
  Dual Ethernet X-Card, 451
  Ethernet ports, 451
  GPS, 454
  LAN network, 452
  mark a section of the log, 329
  port forwarding, 452
  radio module firmware update, 457
  RSR, 466
  SMS, 453
  software and radio firmware updates, 457
  TCP connections, 461
  VPN, 454
  Wi-Fi, 452
  Wi-Fi X-Card, 452
  wireless connection, 456
trusted IPs
  inbound, 177
  outbound, 178

Trusted Phone Number, 212

U

UDP
    Multiple Unicast, 281
UDP connection
    configuring, 286
    settings, 296
update
    ALEOS software, 30
    radio module firmware, 30
USB drivers, installing, 121
USB port, 119

V

VLAN, 146
VPN
    configuration, 155
    GRE, 162
    IPsec, 155, 157
    SSL tunnel, 163
    status, 65
    troubleshooting, 454
VPN 1 tunnel, 157
VRRP, 148

W

WAN/Cellular configuration, 75
WEP encryption, troubleshooting, 452
Wi-Fi
    Access Point Mode, 130
    AP rescan timeout, 139
    Both (AP + Client) Mode, 138
    Client Mode, 134
    configuration, 111
    dual mode, 138
    Landing Page, 197
    modes, 129
    troubleshooting, 452

X

X-Card
    configuration, 290
    Dual Ethernet, 62, 73, 114, 119, 174
    Dual Ethernet, AT command, 390
    Dual Ethernet, troubleshooting, 451
    I/O, 268, 271, 317, 319
    I/O serial port configuration, 290
    I/O, AT command, 442
    Serial port, 71
    status, 48
    type, 48
    Wi-Fi, 111, 115, 152, 197
    Wi-Fi, AT command, 406
    Wi-Fi, troubleshooting, 452

SIERRA
WIRELESS®